Canonical Forms for Matrices over Polynomial Rings

A Thesis Submitted to the
College of Graduate and Postdoctoral Studies
in Partial Fulfillment of the Requirements
for the degree of Master of Science
in the Department of Mathematics and Statistics
University of Saskatchewan
Saskatoon

By
Emmanuel Oluwatobiloba NEYE

Permission to Use

In presenting this thesis in partial fulfilment of the requirements for a Postgraduate degree from the University of Saskatchewan, I agree that the Libraries of this University may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purposes may be granted by the professor or professors who supervised my thesis work or, in their absence, by the Head of the Department or the Dean of the College in which my thesis work was done. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to the University of Saskatchewan in any scholarly use which may be made of any material in my thesis.

Requests for permission to copy or to make other use of material in this thesis in whole or part should be addressed to:

Head of the Department of Mathematics and Statistics
106 Wiggins Road, McLean Hall (Room 142)
University of Saskatchewan
Saskatoon, Saskatchewan S7N 5E6
Canada

OR

Dean
College of Graduate and Postdoctoral Studies
University of Saskatchewan
116 Thorvaldson Building, 110 Science Place
Saskatoon, Saskatchewan S7N 5C9
Canada

Abstract

One of the important concepts in matrix algebra is rank of matrices. If the entries of such matrices are from fields or principal ideal domains, then this concept of rank is well-defined. However, when such matrices are defined over the ring of polynomials $\mathbb{F}[x_1, \ldots, x_k]$, $k \geq 2$ (polynomial matrices in more than one indeterminate), the concept of rank has different but inequivalent definitions. Despite this flaw, some theories, in relation to ranks, can still be applied to polynomial matrices in more than one indeterminate. One of the outcomes of these theories is that lower and upper bounds for ranks of such polynomial matrices in more than one indeterminate can be obtained. Just like matrices over fields or principal ideal domains can be reduced to some simpler or canonical forms, there are algorithms that can be used to reduce matrices over polynomial rings in more than one indeterminate to some simpler forms, though these reduced forms do not always tell the ranks of such polynomial matrices in more than one indeterminate. In this thesis, these algorithms will be presented with examples.

Acknowledgements

I return all glory to God Almighty for His sustenance throughout the period of my study in this reputable university. He is indeed able to do much more, exceeding abundantly, above all one could even ask or think.

I would be highly ungrateful if I do not acknowledge the help, support and contributions of my supervisor while writing this thesis. My profound gratitude goes to him for the fatherly advice he never ceased giving me during my program. Also, I would like to say a very big thank you to him for his financial assistance, in making it possible for me to attend some seminars and conferences. May the good Lord continue to enrich and bless him.

Lastly, I acknowledge the help of the African Institute for Mathematical Sciences (AIMS), South Africa, in making it possible for me to come study in Canada. My coming to study in this university was made possible by God through the post AIMS bursary.

Dedication

This thesis is dedicated to the blessed Trinity: (1) God; the creator of heaven and earth, (2) Jesus; the Son of God and Saviour of the world, and (3) the Holy Spirit; one who will convict the world of sin, of righteousness, and of the coming judgement (John 16:8).

Table of Contents

Permission to Use i

Abstract ii

Acknowledgements iii

Dedication iv

Table of Contents v

List of Figures vi

List of Notation vii

1 Introduction 1

2 Linear Algebra over Principal Ideal Domains 5
- 2.1 Principal ideal domains and Euclidean domains . . . 5
- 2.2 The Euclidean algorithm for GCDs in $\mathbb{Z}$ and $\mathbb{F}[x]$ . . . 11
  - 2.2.1 GCD of two nonzero elements . . . 12
  - 2.2.2 GCD of a finite set of elements . . . 14
- 2.3 Hermite normal form of a matrix over $\mathbb{Z}$ . . . 19
- 2.4 Hermite normal form of a matrix over $\mathbb{F}[x]$ . . . 21

3 Ranks of Matrices over Polynomial Rings 27
- 3.1 Background to the problem . . . 28
  - 3.1.1 Equivalent definitions of the rank of matrices over a field . . . 28
  - 3.1.2 Generic rank of matrices over polynomial rings . . . 31
- 3.2 Determinantal rank . . . 33
  - 3.2.1 Determinants . . . 33
  - 3.2.2 Determinantal rank and determinantal ideals . . . 35
- 3.3 Brief theory of modules in relation to matrix rank . . . 45

4 Analogue of Smith normal form for polynomial matrix 61
- 4.1 Smith normal form of a matrix over $\mathbb{F}[x]$ . . . 61
- 4.2 Partial Smith form of a polynomial matrix . . . 70
- 4.3 Gröbner bases for submodules of R^n, $n \geq 1$, $R = \mathbb{F}[x_1, \ldots, x_k]$ . . . 75
  - 4.3.1 Monomial orderings in R^n . . . 75
  - 4.3.2 Division algorithm in R^n . . . 82
- 4.4 Application of Gröbner bases for submodules of R^n, $n \geq 1$, $R = \mathbb{F}[x_1, \ldots, x_k]$ 98

References 99

List of Figures

2.1 Euclidean algorithm [1, p. 87] 11
2.2 GCD of a finite subset of $\mathbb{Z}$ or $\mathbb{F}[x]$ 17
2.3 Hermite normal form of a matrix over $\mathbb{Z}$ or $\mathbb{F}[x]$ 24
2.3 Hermite normal form of a matrix over $\mathbb{Z}$ or $\mathbb{F}[x]$, continued 25

4.1 Partial Smith form 72
4.2 Division algorithm in R^n 84
4.3 Buchberger's algorithm for submodules in R^n 88
4.4 Submodule Gröbner basis algorithm (matrix form) 97

List of Notation

$\mathbb{F}$	An arbitrary base field, occasionally of characteristic 0
$\mathbb{Q}$	The field of rational numbers
$\mathbb{N}$	The set of positive integers, or the set of natural numbers
$X = \{x_1, \ldots, x_k\}$ $(k \in \mathbb{N})$	A set of k indeterminates
$\mathbb{F}[x]$	The ring of polynomials in one indeterminate x over $\mathbb{F}$
$\mathbb{F}[x_1, \ldots, x_k]$	The ring of polynomials in k indeterminates $x_1, \ldots, x_k$ over $\mathbb{F}$
$\mathbb{Z}_{\geq 0}$	The set of non-negative integers
I_n	$n \times n$ identity matrix
$a \,\vert\, b$	a divides b, or b is divisible by a
$a \nmid b$	a does not divide b, or b is not divisible by a
$\mathrm{LC}\,(f)$	Leading coefficient of a polynomial f
$\mathrm{LT}\,(f)$	Leading term of a polynomial f
$\mathrm{LM}\,(f)$	Leading monomial of a polynomial f
$\mathcal{C}(r, m)$	Set of all *ordered* r-tuples $(i_i, \ldots, i_r)$, where $1 \leq i_1 < i_2 < \cdots < i_r \leq m$
$\overline{f}^G$	The remainder on division of f by elements in the set G

Chapter 1

Introduction

Let $\mathbb{F}$ be a field. $\mathbb{F}[x]$ is the ring of polynomials in one indeterminate over $\mathbb{F}$, and it is a Euclidean domain. Consequently, it is a principal ideal domain (PID), and so given a nonempty subset $S \subseteq \mathbb{F}[x]$ containing at least a nonzero element, there is an element $d \in S$, called the greatest common divisor (GCD) of S, which is just the GCD of all elements in S, and hence a generator for the ideal $\langle S \rangle$ generated by S. In addition, since $\mathbb{F}[x]$ is a Euclidean domain, it becomes possible to compute the GCD of any finite (nonempty and containing at least a nonzero element) subset of $\mathbb{F}[x]$. An algorithm for computing this GCD depends solely on the well known Euclidean algorithm – an algorithm for computing GCD of any two elements in $\mathbb{F}[x]$.

Now, considering a matrix defined over the ring of polynomials $\mathbb{F}[x]$, this matrix can be reduced to a simpler form, called the Hermite normal form, by repeated (but finite) application of the Euclidean algorithm for computing GCD of finite subsets of $\mathbb{F}[x]$. Of course, the Hermite normal form of matrices over $\mathbb{F}[x]$ is the analogue of the row canonical form of matrices over a field. From the Hermite normal form of an arbitrary matrix over $\mathbb{F}[x]$, the rank of such matrix can be obtained, and this is just the number of nonzero rows in the Hermite normal form. In other words, given an $m \times n$ matrix A over $\mathbb{F}[x]$, the submodule of the free $\mathbb{F}[x]$-module $\mathbb{F}[x]^n$ generated by the m rows of matrix A is free, i.e. there exists a finite set of $\mathbb{F}[x]$-linearly independent vectors in $\mathbb{F}[x]^n$ which spans the submodule generated by the m rows of A. However, when it comes to determining rank of matrices over the ring of polynomials in more than one indeterminate, care has to be taken as such rank might not even exist because the submodule might not be free.

Let A be an arbitrary $m \times n$ matrix over $\mathbb{F}[x_1, \ldots, x_k]$, the ring of polynomials in k indeterminates over $\mathbb{F}$. This same matrix A can be regarded as a matrix over $\mathbb{F}(x_1, \ldots, x_k)$, the field of fractions of $\mathbb{F}[x_1, \ldots, x_k]$, and since $\mathbb{F}(x_1, \ldots, x_k)$ is a field, the row (resp. column)

canonical form of matrix A can be computed over $\mathbb{F}(x_1, \ldots, x_k)$, whence the number of nonzero rows (resp. columns) in the resulting matrix after the reduction is called the *generic rank* of the original matrix A. This only gives an upper bound for the rank of a matrix over $\mathbb{F}[x_1, \ldots, x_k]$, and does not tell precisely the rank of such a matrix, if it exists. Another approach of possibly defining ranks of matrices over $\mathbb{F}[x_1, \ldots, x_k]$ is to consider the concept of determinantal rank of polynomial matrices. This concept can be used to determine both lower and upper bounds for ranks of matrices over $\mathbb{F}[x_1, \ldots, x_k]$, but it also does not tell precisely ranks of such matrices.

In order to better understand ranks of matrices over $\mathbb{F}[x_1, \ldots, x_k]$, there is a need to briefly study the theory of modules, in relation to ranks of submodules of some free modules over commutative rings. The ring of polynomials $\mathbb{F}[x_1, \ldots, x_k]$ is a nonzero commutative ring, and so it satisfies the invariant basis number (IBN) property. Consequently, any two (module) bases of an arbitrary free module over $\mathbb{F}[x_1, \ldots, x_k]$ will have the same cardinality. This result is the analogue of one of the main results in linear algebra over a field – any two bases of a vector space over a field have the same cardinality. But of much importance to us is determining in general *ranks* of submodules of free modules over $\mathbb{F}[x_1, \ldots, x_k]$. This is so important since the m rows of an arbitrary $m \times n$ matrix A over $\mathbb{F}[x_1, \ldots, x_k]$ generate a submodule of the free module $\mathbb{F}[x_1, \ldots, x_k]^n$ over $\mathbb{F}[x_1, \ldots, x_k]$, and so seeking for rank of matrix A is similar to determining the rank of the submodule of the free $\mathbb{F}[x_1, \ldots, x_k]$-module generated by the m rows of A. With a very simple example, it can be shown that not every submodule of $\mathbb{F}[x_1, \ldots, x_k]^n$ is free – so not every submodule has a well-defined rank, and also, it can be shown that not every submodule of $\mathbb{F}[x_1, \ldots, x_k]^n$ has a complementary submodule.

Again, given an arbitrary $m \times n$ matrix over $\mathbb{F}[x_1, \ldots, x_k]$, it has earlier been said that the m rows of matrix A generate a submodule of the free $\mathbb{F}[x_1, \ldots, x_k]$-module $\mathbb{F}[x_1, \ldots, x_k]^n$. Gröbner bases for these submodules have been studied in Cox et al[8], and an algorithm for computing such bases exists. It is important to note that these bases (Gröbner bases) need not be linearly independent over $\mathbb{F}[x_1, \ldots, x_k]$, though they span the submodule generated by the m rows of matrix A. As a simple example, when $m = 2$ and $n = 1$, considering the 2×1 matrix $B = \begin{bmatrix} a \\ b \end{bmatrix}$ over $\mathbb{Q}[a, b]$ (where $\mathbb{Q}$ is the field of rational numbers), the set $\{a, b\}$ is a Gröbner basis for the submodule $\langle a, b \rangle \subseteq \mathbb{Q}[a, b]$ generated by the 2 rows of matrix B, which

is just an ideal in $\mathbb{Q}[a, b]$. Obviously, the set $\{a, b\} \subseteq \mathbb{Q}[a, b]$ is not linearly independent over $\mathbb{Q}[a, b]$ due to the relation $b \cdot a - a \cdot b = 0$.

In this thesis, some algorithms will be given – algorithms for reducing matrices over the ring of polynomials $\mathbb{F}[x_1, \ldots, x_k]$, $k \geq 2$ into some simpler forms or even canonical forms. Sometimes, this simpler form can tell if the submodule generated by the rows of the original matrices is free, and consequently, the rank of the original matrices can be determined.

Chapter 2 of this thesis gives a very concise overview of linear algebra over PIDs. In this chapter, the Euclidean algorithm for computing GCD of any two elements in R (where R is either $\mathbb{Z}$, the ring of integers, or $\mathbb{F}[x]$, the polynomial ring in one indeterminate over a field) is extended to computing the GCD of any finite subset of R. These concepts play major role in proving the existence and uniqueness of the Hermite normal form of matrices over R. Lastly, algorithms for computing the Hermite normal form of matrices over R are given. The main references used for the materials in this chapter are Adkins and Weintraub [1], and Bremner and Peresi [4].

Chapter 3 talks extensively about ranks of matrices over the ring of polynomials $\mathbb{F}[x_1, \ldots, x_k]$. This chapter starts with a brief description of the ring of polynomials in k indeterminates. The rest of the chapter focuses on extending, in particular, the concept of ranks from linear algebra over a field, to linear algebra over the ring of polynomials $\mathbb{F}[x_1, \ldots, x_k]$. Some definitions of ranks of matrices over a field are considered, and all these definitions are equivalent. The generic rank of matrices over polynomial rings $\mathbb{F}[x_1, \ldots, x_k]$ is defined, with an example given for better understanding. After this, the theory of determinantal rank, in relation to ranks of matrices over polynomial rings $\mathbb{F}[x_1, \ldots, x_k]$, is discussed. Lastly, in order for ranks of matrices over $\mathbb{F}[x_1, \ldots, x_k]$ to be better understood, a brief theory of modules is discussed, in relation to ranks of matrices over $\mathbb{F}[x_1, \ldots, x_k]$, and at the end, a very simple example is given to show that not every submodule of a free module is free. The primary references used for the materials in this chapter are Adkins and Weintraub [1], and Hoffman and Kunze [12].

In Chapter 4, which is the last chapter, the Smith normal form of matrices over the Euclidean domain $\mathbb{F}[x]$ is first defined. Next to this, some results that help in proving the existence and uniqueness of this Smith normal form are given, with their proofs. The concept

of Smith normal form is then extended to reducing *some* matrices over the polynomial rings $\mathbb{F}[x_1, \ldots, x_k]$, $k \geq 2$ into a simpler form called *partial Smith form* [3]. Lastly, in general, the theory of Gröbner basis for submodules of free $\mathbb{F}[x_1, \ldots, x_k]$-modules $\mathbb{F}[x_1, \ldots, x_k]^n$ is discussed, with examples given for better understanding. The major references used for the materials in this chapter are Norman [18], Bremner and Dotsenko [3], and Cox et el. [7, 8].

Chapter 2

Linear Algebra over Principal Ideal Domains

A **ring** is a nonempty set R equipped with two binary operations $+$ and $\cdot$, such that $(R, +)$ is an abelian (commutative) group, $\cdot$ is associative (i.e. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$), and $\cdot$ is distributive over $+$ (i.e. $a \cdot (b+c) = a \cdot b + a \cdot c$, and $(a+b) \cdot c = a \cdot c + b \cdot c$, for all $a, b, c \in R$). If $a \cdot b = b \cdot a$ for all $a, b \in R$, then $(R, +, \cdot)$ is a **commutative ring**. If in addition there exists an element $e \in R$ such that $a \cdot e = e \cdot a = a$ for all $a \in R$, then $(R, +, \cdot)$ is a **commutative ring with identity (or commutative unital ring)**. Of much interest to us in this chapter is a particular type of ring called principal ideal domain. An **integral domain** is a commutative ring R with identity such that for all $a, b \in R$, $a \cdot b = 0$ implies $a = 0$ or $b = 0$. An integral domain R in which every ideal in R can be generated by a single element of R is called a **principal ideal domain** (PID). More often, we will write ab instead of $a \cdot b$, where $\cdot$ has been omitted. The primary reference in this chapter is Adkins and Weintraub [1].

2.1 Principal ideal domains and Euclidean domains

There is a relationship between principal ideal domains and Euclidean domains: every Euclidean domain is a principal ideal domain, but the reverse is not always true. In this section, principal ideal domain and Euclidean domain will be briefly studied, and examples will be given for better understanding. More study relating to PIDs and Euclidean domains can be found in [1] (Chapter 2, Section 5).

Definition 2.1.1. Let $(R, +, \cdot)$ be a commutative ring and I be a subset of R. I is said to be an **ideal** of R if the following conditions are satisfied:

(1) $(I, +)$ is a subgroup of $(R, +)$, i.e. $a - b \in I$ for all $a, b \in I$.

(2) $ra \in I$, for all $a \in I$ and for all $r \in R$.

Definition 2.1.2. Let R be a commutative unital ring. An ideal $I \subseteq R$ is said to be **principal** if there exists an element $a \in R$ such that $I = Ra = \{ra : r \in R\}$. R is said to be a **principal ideal domain (PID)** if every ideal of R is of the form Ra for some $a \in R$, i.e. if every ideal of R is generated by a single element of R. If $I \subseteq R$ is generated by a single element $a \in R$, we write $I = \langle a \rangle$, i.e. $Ra = \langle a \rangle$.

Example 2.1.3. Some examples of principal ideal domains are any field $\mathbb{F}$ (since only ideals are $\{0\}$ and $\mathbb{F}$ itself), the ring of integers, $\mathbb{Z}$, and the polynomial ring $\mathbb{F}[x]$, where $\mathbb{F}$ is a field.

Definition 2.1.4. Let R be an integral domain. A nonzero element $a \in R$ is said to be a **divisor** of an element $b \in R$ (or b is **divisible** by a) if there exists an element $c \in R$ such that $b = ac$. If a is a divisor of b, we say a **divides** b, written $a \,|\, b$. A **common divisor** for a nonempty subset S of R is an element $d \in R$ such that $d \,|\, s$ for all $s \in S$.

Definition 2.1.5. Let R be an integral domain and S be a subset of R with at least one nonzero element. A **greatest common divisor** of S, denoted $\gcd(S)$, is an element $d \in R$ such that d is a common divisor of S, and if another element $d' \in R$ is a common divisor of S, then $d' \,|\, d$.

Theorem 2.1.6. *Let R be a principal ideal domain and S be a subset of R, containing at least one nonzero element. Then an element $d \in S$ is a greatest common divisor of S (i.e. $d = \gcd(S)$) if and only if d is the generator of $\langle S \rangle$, the ideal generated by S (i.e. $\langle d \rangle = \langle S \rangle$).*

Proof. Though the proof that will be given here is basically the same as proof of the first part of Theorem 2.5.6 in Adkins & Weintraub [1], more details are being given here.

Suppose that an element $d \in R$ equals $\gcd(S)$. First, d being greatest common divisor of S implies by definition that d is a common divisor of s_i for all $s_i \in S$. That is, for every $s_i \in S$, s_i equals da_i for some $a_i \in R$. Let t be any element in $\langle S \rangle$. Then t can be written in the form $\sum_{i=1}^{n} b_i s_i$ for some $b_i \in R$, $s_i \in S$ and $n \geq 1$. Thus, $t = \sum_{i=1}^{n} b_i s_i = \sum_{i=1}^{n} b_i (da_i) = \left(\sum_{i=1}^{n} b_i a_i \right) d$, implying t belongs to $\langle d \rangle$, since $\sum_{i=1}^{n} b_i a_i$ belongs to R. Hence, $\langle S \rangle \subseteq \langle d \rangle$. Also, there exists an integer d' such that $\langle S \rangle$ equals $\langle d' \rangle$, reason being that R is a principal ideal domain. It will now be shown that $\langle d \rangle$ is contained in $\langle S \rangle = \langle d' \rangle$. Since $\langle S \rangle$ equals $\langle d' \rangle$, it implies every element of S belongs to $\langle d' \rangle$, and so d' is a common divisor of all elements in

S. Since d is a greatest common divisor of S, it implies d' divides d by definition 2.1.4, i.e. d belongs to $\langle d' \rangle = \langle S \rangle$, as expected. That is, $\langle d \rangle \subseteq \langle S \rangle$. Hence, $\langle d \rangle = \langle S \rangle$.

Conversely, suppose that for some $d \in R$, $\langle d \rangle$ equals $\langle S \rangle$. For all $s_i \in S$, s_i belongs to $\langle S \rangle = \langle d \rangle$, i.e. d is a common divisor of s_i for all $s_i \in S$. Let d' be another common divisor of s_i for all $s_i \in S$. Then $s_i = d'b_i$ for some $b_i \in R$. Since $\langle d \rangle$ equals $\langle S \rangle$, it implies d belongs to $\langle S \rangle$, and so d can be written in the form $\sum_{i=1}^{n} c_i s_i$ for some $c_i \in R$, $s_i \in S$ and $n \geq 1$. Thus, $d = \sum_{i=1}^{n} c_i s_i = \sum_{i=1}^{n} c_i (d' a_i) = \left(\sum_{i=1}^{n} c_i a_i \right) d'$, implying d belongs to $\langle d' \rangle$, i.e. d' divides d. Hence, by definition 2.1.4, d is the greatest common divisor of S. □

The next theorem is the well known **division algorithm**. Though the result will be stated in two versions: one over the ring of integers, $\mathbb{Z}$ and the other over the ring of polynomials $\mathbb{F}[x]$ in one indeterminate with coefficients in a field, only the latter will be proved.

Theorem 2.1.7. *Let b be any nonzero element in $\mathbb{Z}$. Then for any integer $a \in \mathbb{Z}$, there exist unique integers q and r such that $a = bq + r$, where $0 \leq r < |b|$ ($|b|$ is the absolute value of b).*

Definition 2.1.8. Let f be a nonzero element in $\mathbb{F}[x]$, where $\mathbb{F}$ is a field. Then f can be written as $f = \sum_{i=0}^{m} a_i x^i$, where a_i $(0 \leq i \leq m)$ is an element in $\mathbb{F}$.

(1) If $a_m \neq 0$, then m is the **degree** of f, denoted $\deg(f) = m$.

(2) If $\deg(f) = m$, then $a_m x^m$ is the **leading term** of f, denoted $\mathrm{LT}(f) = a_m x^m$.

(3) If $\mathrm{LT}(f) = a_m x^m$, then a_m is the **leading coefficient** of f, denoted $\mathrm{LC}(f) = a_m$.

(4) If $\mathrm{LT}(f) = a_m x^m$, then x^m is the **leading monomial** of f, denoted $\mathrm{LM}(f) = x^m$.

Theorem 2.1.9. *Let g be any nonzero polynomial in $\mathbb{F}[x]$. Then for any polynomial $f \in \mathbb{F}[x]$, there exist unique polynomials q and r in $\mathbb{F}[x]$ such that $f = qg + r$, where either $r = 0$ or $\deg(r) < \deg(g)$.*

Proof. The proof of this theorem has two parts: the existence of q and r, and their uniqueness. Hungerford [14] used induction to show the existence part of this result (Theorem 4.4); but here instead, it is proven by contradiction. To this end, let f and g be polynomials in $\mathbb{F}[x]$, where g is nonzero.

Existence of q and r: If $g \mid f$, then there exists $q \in \mathbb{F}[x]$ such that $f = qg$, so we take $r = 0$ and that completes the first part of the proof. Thus, we can assume $g \nmid f$ (so $f \neq 0$) and let

$$S = \big\{ f - qg \neq 0 \,:\, q \in \mathbb{F}[x] \big\}.$$

This set S is a nonempty subset of $\mathbb{F}[x]$, and by the well-ordering principle on the set of degrees of polynomials in S, there exists a polynomial $r \in S$ of least degree. Thus, $r = f - qg$ for some $q \in \mathbb{F}[x]$. Let $\deg(r) = m$ and $\deg(g) = n$, i.e. $r = \sum_{i=0}^{m} a_i x^i$ $(a_m \neq 0)$ and $g = \sum_{j=0}^{n} b_j x^j$ $(b_n \neq 0)$. We will show that $m < n$. Assume to the contrary that $m \geq n$; multiplying g by $\frac{a_m}{b_n}\, x^{m-n}$ and then subtracting the product from r, we obtain:

$$r_1 = r - \frac{a_m}{b_n}\, x^{m-n}\, g.$$

From the last equation, we see that either $r_1 = 0$ or $\deg(r_1) < \deg(r)$. If $r_1 = 0$, then $r = \frac{a_m}{b_n}\, x^{m-n}\, g$, and so

$$r = f - qg \implies \frac{a_m}{b_n}\, x^{m-n}\, g = f - qg \implies f = \frac{a_m}{b_n}\, x^{m-n}\, g + qg = \left(\frac{a_m}{b_n}\, x^{m-n} + q \right) g,$$

i.e. $g \mid f$, a contradiction. If $r_1 \neq 0$, then $\deg(r_1) < \deg(r)$, and so

$$r = f - qg \implies r_1 + \frac{a_m}{b_n}\, x^{m-n}\, g = f - qg \implies r_1 = f - \left(q + \frac{a_m}{b_n}\, x^{m-n} \right) g,$$

i.e. r_1 belongs to S (where $\deg(r_1) < \deg(r)$), a contradiction on choice of r as polynomial in S of least degree. Hence, $m < n$, i.e. $\deg(r) < \deg(g)$.

Uniqueness of q and r: Suppose for polynomials f and g in $\mathbb{F}[x]$, there exists polynomials q, q', r, r' in $\mathbb{F}[x]$ such that $qg + r = f = q'g + r'$ where either $r = 0$ or $\deg(r) < \deg(g)$, and either $r' = 0$ or $\deg(r') < \deg(g)$. First, that either $r = 0$ or $\deg(r) < \deg(g)$, and either $r' = 0$ or $\deg(r') < \deg(g)$, both imply either $r - r' = 0$ or $\deg(r - r') < \deg(g)$. That $qg + r = f = q'g + r'$ implies $g(q - q') = r' - r$, i.e. if $r' - r \neq 0$, we will have $\deg(r' - r) = \deg\big(g(q - q')\big) = \deg(g) + \deg(q - q') \geq \deg(g)$, i.e. $\deg(r' - r) \geq \deg(g)$, a contradiction since $\deg(r - r') < \deg(g)$. Hence, $r' - r = 0$, i.e. $r' = r$. This further implies $g(q - q') = 0$, i.e. $q - q' = 0$ since $g \neq 0$, i.e. $q = q'$.

This completes the proof. $\square$

Definition 2.1.10. [1, p. 86] Let R be an integral domain and $\mathbb{Z}_{\geq 0}$ be the set of non-negative integers. R is said to be a **Euclidean domain** if there exists a function $\phi : R\backslash\{0\} \longrightarrow \mathbb{Z}_{\geq 0}$, called a **Euclidean function**, such that the following are satisfied:

(1) For all $a, b \in R\backslash\{0\}$, $\phi(a) \leq \phi(ab)$.

(2) For all $a \in R$ and $b \in R\backslash\{0\}$, there exist $q, r \in R$ such that $a = bq + r$, where either $r = 0$ or $\phi(r) < \phi(b)$.

Example 2.1.11. Some examples of Euclidean domains are:

(1) The ring of integers, $\mathbb{Z}$ with Euclidean function $\phi(a) = |a|$, for all nonzero integers a, where $|a|$ is the absolute value of a.

(2) The ring of polynomials $\mathbb{F}[x]$ ($\mathbb{F}$, being a field) with Euclidean function $\phi(f) = \deg(f)$, for all nonzero polynomials f.

The next result shows that all Euclidean domains are principal ideal domains; however, the converse is not always true.

Theorem 2.1.12. *Let R be a Euclidean domain. Then R is a principal ideal domain.*

Proof. For the proof of this theorem, we follow the argument of Adkins & Weintraub [1] (Theorem 2.5.19), just that here there is a change of notation. Let R be a Euclidean domain with its Euclidean function ϕ. If I is a zero ideal of R, then $I = \{0\} = \langle 0\rangle$, and so is principal. Let I be a nonzero ideal of R and set $S := \big\{\phi(a) : a \in I\backslash\{0\}\big\}$, a subset of non-negative integers, $\mathbb{Z}_{\geq 0}$. By the well-ordering principle on $\mathbb{Z}_{\geq 0}$, the set $S \subseteq \mathbb{Z}_{\geq 0}$ has a least element, say $\phi(b)$. It will be shown that the ideal I is generated by the nonzero element $b \in I$, i.e. $I = Rb = \langle b\rangle$. First, since b belongs to I, it implies by definition of ideal that rb belongs to I for all $r \in R$, i.e. $Rb \subseteq I$. On the other hand, if a belongs to I, then by condition (2) of definition 2.1.10, there exists $q, r \in R$ such that $a = bq + r$, where either $r = 0$ or $\phi(r) < \phi(b)$. From $a = bq + r$, it follows that $r = a - bq$ belongs to I since both a and bq are in I, I being an ideal. If r does not equal 0 ($r \neq 0$), then by the choice of $\phi(b)$, it implies that $\phi(b) \leq \phi(r)$, a contradiction. Hence, $r = 0$ and so $a = bq$, i.e. a belongs to $\langle b\rangle = Rb$, i.e. $I \subseteq Rb$. Therefore, $I = Rb$, and so R is a principal ideal domain. □

Remark 2.1.13. The reverse of the theorem above does not always hold. For example, though the ring $\mathbb{R}[x,y]/\langle x^2+y^2+1\rangle$, where $\mathbb{R}$ is the field of real numbers, is a principal ideal domain, it is not a Euclidean domain. This example is one of the non-Euclidean PIDs stated on the Euclidean domain page of Wikipedia (`https://en.wikipedia.org/wiki/Euclidean_domain#Examples`), but without a reference. Though it is an interesting example since it has to do with a polynomial, I was unable to completely show it is indeed a non-Euclidean PID. Another example of a non-Euclidean PID is the ring

$$R = \left\{ a + b\theta \,:\, a, b \in \mathbb{Z},\, \theta = \frac{1+\sqrt{-19}}{2} \right\}.$$

Wilson [20] showed that the just mentioned ring is indeed a non-Euclidean PID.

It is important to note that since Euclidean domains have been shown to be principal ideal domains, the concept of greatest common divisor does exist in Euclidean domains. The Euclidean Algorithm will be stated below as Algorithm 2.1, but before doing this, there is a need to state a lemma; a basic result which helps establish that $r_n = \gcd(a,b)$ in Algorithm 2.1. This result is a claim, stated and proved, on page 87 of Adkins and Weintraub [1].

Lemma 2.1.14. *Let R be a principal ideal domain and let a and b be elements of R such that $a = bq + r$ for some $q, r \in R$. Then* $\gcd\big(\{a,b\}\big) = \gcd\big(\{b,r\}\big)$.

Proof. Let a, b and r be elements in R. Considering the subsets $\{a,b\}$ and $\{b,r\}$ of R, R being a principal ideal domain, it follows from Theorem 2.1.6 that $d_1 = \gcd\big(\{a,b\}\big)$ and $d_2 = \gcd\big(\{b,r\}\big)$, where d_1 and d_2 are the generators of ideals $\langle a,b\rangle$ and $\langle b,r\rangle$, respectively. So in order to show that $d_1 = d_2$, it suffices to show that $\langle a,b\rangle = \langle b,r\rangle$. To this end, let c be an element in $\langle a,b\rangle$. Then $c = aa' + bb'$ for some $a', b' \in R$, and since $a = bq + r$, it follows that c belongs to $\langle b,r\rangle$, reason being that $c = (bq+r)a' + bb' = b(qa'+b') + ra'$. Hence, $\langle a,b\rangle \subseteq \langle b,r\rangle$. Similarly, if c is an element in $\langle b,r\rangle$, then $c = bb' + rr'$ for some $b', r' \in R$, and since $a = bq+r$, it follows that $c = bb' + (a-bq)r' = ar' + b(b'-qr')$, i.e. c belongs to $\langle a,b\rangle$, so that $\langle b,r\rangle \subseteq \langle a,b\rangle$. Therefore, $\langle a,b\rangle = \langle b,r\rangle$, i.e. $\gcd\big(\{a,b\}\big) = d_1 = d_2 = \gcd\big(\{b,r\}\big)$. □

Now, let R be a Euclidean domain with ϕ as its Euclidean function. If a and b are nonzero elements in R, then there is an algorithm called the Euclidean algorithm, for computing the greatest common divisor of a and b, denoted $\gcd(a,b)$. Assuming $\phi(b) < \phi(a)$, Algorithm 2.1 is an algorithm for computing $\gcd(a,b)$. If $b = 0$, then $\gcd(a,b) = a$.

$$
\begin{array}{lll}
a = bq_1 + r_1 & \text{where} & \phi(r_1) < \phi(b) \\
b = r_1q_2 + r_2 & \text{where} & \phi(r_2) < \phi(r_1) \\
r_1 = r_2q_3 + r_3 & \text{where} & \phi(r_3) < \phi(r_2) \\
\vdots & \vdots & \vdots \\
r_{n-2} = r_{n-1}q_n + r_n & \text{where} & \phi(r_n) < \phi(r_{n-1}) \\
r_{n-1} = r_nq_{n+1} + r_{n+1} & \text{where} & r_{n+1} = 0
\end{array}
$$

Algorithm 2.1: Euclidean algorithm [1, p. 87]

It is first important to note that the above algorithm does terminate after a finite number of steps; reason being that $\phi(r_1) > \phi(r_2) > \phi(r_3) > \cdots$ is a strictly decreasing sequence of elements of $\mathbb{Z}_{\geq 0}$. In other words, there exists a natural number n such that $r_n \neq 0$, but $r_{n+1} = 0$.

Furthermore, considering the first line of the above algorithm, it says $a = bq_1 + r_1$, implying by Lemma 2.1.14 that $\gcd(a, b) = \gcd(b, r_1)$. Similarly, $\gcd(b, r_1) = \gcd(r_1, r_2)$ from the second line of the same algorithm. Also, $\gcd(r_1, r_2) = \gcd(r_2, r_3)$ from the third line. Lastly, just before the last line of the algorithm, it follows that $\gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n)$. However, the last line of the algorithm implies $\gcd(r_{n-1}, r_n) = r_n$ since r_{n-1} is a multiple of r_n. Therefore,

$$r_n = \gcd(r_{n-1}, r_n) = \gcd(r_{n-2}, r_{n-1}) = \cdots = \gcd(r_2, r_3) = \gcd(r_1, r_2) = \gcd(b, r_1) = \gcd(a, b).$$

2.2 The Euclidean algorithm for GCDs in $\mathbb{Z}$ and $\mathbb{F}[x]$

In this section, R will stand for either the ring of integers, $\mathbb{Z}$, or the ring of polynomials in one inderterminate, $\mathbb{F}[x]$, where $\mathbb{F}$ is a field. In this subsection, Algorithm 2.1 will be translated to matrix elementary row operations, and thereafter, this algorithm will be extended to computing GCDs of finite subsets of R.

2.2.1 GCD of two nonzero elements

Following strictly Algorithm 2.1, let

$$A = \begin{bmatrix} a_{11} \\ a_{21} \end{bmatrix}$$

be a 2×1 matrix over R, where a_{11} and a_{21} are nonzero. Assuming $\phi(a_{11}) < \phi(a_{21})$, then by Theorem 2.1.7 or Theorem 2.1.9, there exists q_1 and r_1 in R such that $a_{21} = a_{11}q_1 + r_1$ where $r_1 = 0$ or $\phi(r_1) < \phi(a_{11})$. Thus, multiplying row 1 of matrices A and I_2 (the 2×2 identity matrix) by $-q_1$ and then adding the result to row 2 of respective matrices, we obtain the matrices

$$A_1 = \begin{bmatrix} a_{11} \\ r_1 \end{bmatrix} \qquad \text{and} \qquad U_1 = \begin{bmatrix} 1 & 0 \\ -q_1 & 1 \end{bmatrix},$$

where U_1 is the elementary matrix corresponding to multiplying row 1 of matrix A by $-q_1$ and then adding the result to row 2, i.e. $U_1A = A_1$.

If $r_1 = 0$, then $\gcd(a_{11}, a_{21}) = a_{11}$. Otherwise, $\phi(r_1) < \phi(a_{11})$, and so we interchange the rows of matrix A_1, yielding the matrices

$$A_1' = \begin{bmatrix} r_1 \\ a_{11} \end{bmatrix} \qquad \text{and} \qquad U' = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

where U' is the elementary matrix corresponding to interchanging rows 1 and 2 of matrix A_1, i.e. $U'A_1 = A_1'$. Similarly, there exists q_2 and r_2 in R such that $a_{11} = r_1q_2 + r_2$ where $r_2 = 0$ or $\phi(r_2) < \phi(r_1)$. Thus, multiplying row 1 of both matrices A_1' and I_2 by $-q_2$ and then adding the result to row 2 of respective matrices, give the matrices

$$A_2 = \begin{bmatrix} r_1 \\ r_2 \end{bmatrix} \qquad \text{and} \qquad U_2 = \begin{bmatrix} 1 & 0 \\ -q_2 & 1 \end{bmatrix},$$

i.e. $U_2A_1' = A_2$.

Similarly, if $r_2 = 0$, then $\gcd(a_{11}, a_{21}) = r_1$. Otherwise, rows of matrix A_2 are interchanged, yielding the matrices

$$A_2' = \begin{bmatrix} r_2 \\ r_1 \end{bmatrix} \qquad \text{and} \qquad U' = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

i.e. $U'A_2 = A_2'$. Furthermore, there exists q_3 and r_3 in R such that $r_1 = r_2q_3 + r_3$ where $r_3 = 0$ or $\phi(r_3) < \phi(r_2)$. Thus, multiplying row 1 of both matrices A_2' and I_2 by $-q_3$ and then adding the result to row 2 of respective matrices, give the matrices

$$A_3 = \begin{bmatrix} r_2 \\ r_3 \end{bmatrix} \qquad \text{and} \qquad U_3 = \begin{bmatrix} 1 & 0 \\ -q_3 & 1 \end{bmatrix},$$

i.e. $U_3A_2' = A_3$.

Continuing this way a finite number of times, we obtain matrices

$$A_n' = \begin{bmatrix} r_n \\ r_{n-1} \end{bmatrix}, \qquad A_{n+1} = \begin{bmatrix} r_n \\ 0 \end{bmatrix} \qquad \text{and} \qquad U_{n+1} = \begin{bmatrix} 1 & 0 \\ -q_{n+1} & 1 \end{bmatrix},$$

where $U_{n+1}A_n' = A_{n+1}$. Taking U as the product of the elementary matrices U_{n+1}, U', U_n, $\ldots$, U', U_2, U' and U_1, i.e. $U = U_{n+1}\,U'\,U_n \cdots U'\,U_2\,U'\,U_1$, we obtain

$$UA = A_{n+1} = \begin{bmatrix} r_n \\ 0 \end{bmatrix}.$$

Lemma 2.2.1. *Let A be a nonzero 2×1 matrix over R and d be the greatest common divisor of A (i.e. $d = \gcd(A)$). Then there is an invertible matrix U over R (U is a product of some elementary matrices over R) such that*

$$UA = \begin{bmatrix} d \\ 0 \end{bmatrix}.$$

Proof. The above discussion is a constructive proof. □

Example 2.2.2. Let

$$A = \begin{bmatrix} 628 & 188 \end{bmatrix}^t$$

be a 2×1 matrix over $\mathbb{Z}$. We obtain the following:

$$\begin{bmatrix} 628 \\ 188 \end{bmatrix} \xrightarrow{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}} \begin{bmatrix} 188 \\ 628 \end{bmatrix} \xrightarrow{\begin{bmatrix} 1 & 0 \\ -3 & 1 \end{bmatrix}} \begin{bmatrix} 188 \\ 64 \end{bmatrix} \xrightarrow{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}} \begin{bmatrix} 64 \\ 188 \end{bmatrix} \xrightarrow{\begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix}} \begin{bmatrix} 64 \\ 60 \end{bmatrix}$$

$$\begin{bmatrix} 64 \\ 60 \end{bmatrix} \xrightarrow{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}} \begin{bmatrix} 60 \\ 64 \end{bmatrix} \xrightarrow{\begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}} \begin{bmatrix} 60 \\ 4 \end{bmatrix} \xrightarrow{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}} \begin{bmatrix} 4 \\ 60 \end{bmatrix} \xrightarrow{\begin{bmatrix} 1 & 0 \\ -15 & 1 \end{bmatrix}} \begin{bmatrix} 4 \\ 0 \end{bmatrix}.$$

Setting

$$U = \begin{bmatrix} 1 & 0 \\ -15 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -3 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 3 & -10 \\ -47 & 157 \end{bmatrix},$$

it follows that $UA = \begin{bmatrix} 4 & 0 \end{bmatrix}^t$. In other words, $\gcd(628, 188) = 4$.

2.2.2 GCD of a finite set of elements

In this subsection, a method for computing the greatest common divisor (GCD) of a finite subset of R ($\mathbb{Z}$ or $\mathbb{F}[x]$) (with at least one nonzero element) will be discussed, and at the center of this discussion is the application of Algorithm 2.1. In other words, Algorithm 2.1 can be extended to compute the GCD of any finite set of elements in R, and this extension can be expressed conveniently in terms of row operations on a column vector. Algorithm 2.2 is just the algorithm for computing the GCD of a column vector, and it is the inner loop (b) of Figure 1 (Algorithm for the Hermite normal form) in [4].

Let

$$A = \begin{bmatrix} a_{11} & a_{21} & \cdots & a_{m1} \end{bmatrix}^t$$

be an $m \times 1$ matrix over R, where at least one a_{i1} $(1 \leq i \leq m)$ is nonzero. Let

$$L = \begin{cases} \left\{ |a_{i1}| \,:\, a_{i1} \neq 0,\ 1 \leq i \leq m \right\} & \text{if } R = \mathbb{Z} \\ \left\{ \deg\left(a_{i1}\right) \,:\, a_{i1} \neq 0,\ 1 \leq i \leq m \right\} & \text{if } R = \mathbb{F}[x] \end{cases}$$

and set least_position$(A) := k$ where

$$k = \begin{cases} \min\left\{ i \,:\, |a_{i1}| = \min L,\ 1 \leq i \leq m \right\} & \text{if } R = \mathbb{Z} \\ \min\left\{ i \,:\, \deg\left(a_{i1}\right) = \min L,\ 1 \leq i \leq m \right\} & \text{if } R = \mathbb{F}[x] \end{cases}.$$

Interchanging rows 1 and k of matrix A gives matrix

$$A' = \begin{bmatrix} a_{k1} & a_{21} & \cdots & a_{11} & \cdots & a_{n1} \end{bmatrix}^t, \text{ relabelled as } A' = \begin{bmatrix} a_{11} & a_{21} & \cdots & a_{n1} \end{bmatrix}^t.$$

Let U' be the elementary matrix over R obtained by interchanging rows 1 and k of matrix A. Then $U'A = A'$. Now, using Theorem 2.1.7 or Theorem 2.1.9, there exists $q_{i1}^{(1)}$ and $r_{i1}^{(1)}$ $(2 \leq i \leq m)$ in R such that for all i $(2 \leq i \leq m)$, $a_{i1} = a_{11}q_{i1}^{(1)} + r_{i1}^{(1)}$ where $r_{i1}^{(1)} = 0$ or

$\phi(r_{i1}^{(1)}) < \phi(a_{11})$. Thus, for each i $(2 \leq i \leq m)$, setting $A_1 := A'$ and then adding $-q_{i1}^{(1)}$ times row 1 of matrix A' to row i of A', we obtain the matrix

$$A_1 = \begin{bmatrix} a_{11} & r_{21}^{(1)} & \cdots & r_{n1}^{(1)} \end{bmatrix}^t.$$

For each of the last $m-1$ elementary operations performed before we finally obtain matrix A_1, if U_{i1} $(2 \leq i \leq m)$ is the corresponding elementary matrix, then $U_1 A' = A_1$, where $U_1 = U_{n1} \cdots U_{31} U_{21}$.

If $r_{i1}^{(1)} = 0$ for all i $(2 \leq i \leq m)$, then $\gcd(A) = a_{11}$. Otherwise, set

$$L := \begin{cases} \left\{ |r_{i1}^{(1)}| \, : \, r_{i1}^{(1)} \neq 0, \ 2 \leq i \leq m \right\} & \text{if } \ R = \mathbb{Z} \\ \left\{ \deg\left(r_{i1}^{(1)}\right) \, : \, r_{i1}^{(1)} \neq 0, \ 2 \leq i \leq m \right\} & \text{if } \ R = \mathbb{F}[x] \end{cases}$$

and least_position$(A_1) := k$ where

$$k = \begin{cases} \min\left\{ i \, : \, |r_{i1}^{(1)}| = \min L, \ 2 \leq i \leq m \right\} & \text{if } \ R = \mathbb{Z} \\ \min\left\{ i \, : \, \deg\left(r_{i1}^{(1)}\right) = \min L, \ 2 \leq i \leq m \right\} & \text{if } \ R = \mathbb{F}[x] \end{cases}.$$

Interchanging rows 1 and k of matrix A_1 gives the matrix

$$A_1' = \begin{bmatrix} r_{k1}^{(1)} & r_{21}^{(1)} & \cdots & a_{11} & \cdots & r_{n1}^{(1)} \end{bmatrix}^t, \text{ relabelled as } A_1' = \begin{bmatrix} r_{11}^{(1)} & r_{21}^{(1)} & \cdots & r_{n1}^{(1)} \end{bmatrix}^t.$$

If U_1' is the elementary matrix over R obtained by interchanging rows 1 and k of matrix A_1, then $U_1' A_1 = A_1'$. Similarly, by Theorem 2.1.7 or Theorem 2.1.9, there exists $q_{i1}^{(2)}$ and $r_{i1}^{(2)}$ $(2 \leq i \leq m)$ in R such that for all i $(2 \leq i \leq m)$, $r_{i1}^{(1)} = r_{11}^{(1)} q_{i1}^{(2)} + r_{i1}^{(2)}$ where $r_{i1}^{(2)} = 0$ or $\phi(r_{i1}^{(2)}) < \phi(r_{11}^{(1)})$. Thus, for each i $(2 \leq i \leq m)$, setting $A_2 := A_1'$ and then adding $-q_{i1}^{(2)}$ times row 1 of matrix A_1' to row i of A_1', we obtain the matrix

$$A_2 = \begin{bmatrix} r_{11}^{(1)} & r_{21}^{(2)} & \cdots & r_{n1}^{(2)} \end{bmatrix}^t.$$

For each of the last $m-1$ elementary operations performed before we finally obtain matrix A_2, if U_{i2} $(2 \leq i \leq m)$ is the corresponding elementary matrix, then $U_2 A_1' = A_2$, where $U_2 = U_{n2} \cdots U_{32} U_{22}$.

If $r_{i1}^{(2)} = 0$ for all i $(2 \leq i \leq m)$, then $\gcd(A) = r_{11}^{(1)}$. Otherwise, the same procedure as above is repeated (for a finite number of times) until we obtain a matrix of the form

$$A_{n+1} = \begin{bmatrix} d & 0 & \cdots & 0 \end{bmatrix}^t.$$

The procedure described above does terminate. For example, considering the first two iterations performed above, where $r_{i1}^{(1)} = 0$ or $\phi(r_{i1}^{(1)}) < \phi(a_{11})$ $(2 \leq i \leq m)$ and $r_{i1}^{(2)} = 0$ or $\phi(r_{i1}^{(2)}) < \phi(r_{11}^{(1)})$ $(2 \leq i \leq m)$, we observe that $r_{i1}^{(2)} = 0$ or $\phi(r_{i1}^{(2)}) < \phi(r_{11}^{(1)}) < \phi(a_{11})$ $(2 \leq i \leq m)$, implying that (non-negative) upper bounds for the remainders ($r_{i1}^{(1)}$ and $r_{i1}^{(2)}$, $2 \leq i \leq m$) gotten in the first two iterations performed above are getting smaller and smaller. Continuing the procedure (for a finite number of steps), we will eventually get to a point where all remainders will be zero. The above procedure is summarized in Algorithm 2.2.

Lemma 2.2.3. *Let A be a nonzero $m \times 1$ matrix over R and d be the greatest common divisor of A (i.e. $d = \gcd(A)$). Then there is an invertible matrix U over R (U is a product of some elementary matrices over R) such that*

$$UA = \begin{bmatrix} d & 0 & \cdots & 0 \end{bmatrix}^t.$$

Proof. This follows from the above discussion and Algorithm 2.2. □

Remark 2.2.4. Let B be a nonzero $1 \times n$ matrix over R ($\mathbb{Z}$ or $\mathbb{F}[x]$) . Then the transpose B^t of B is a nonzero $n \times 1$ matrix over R. If the GCD of B^t is d, then by Lemma 2.2.3, there exists an invertible matrix U over R such that

$$UB^t = \begin{bmatrix} d & 0 & \cdots & 0 \end{bmatrix}^t.$$

Taking the transpose of both sides of the last equation, yields

$$BU^t = \begin{bmatrix} d & 0 & \cdots & 0 \end{bmatrix}.$$

Summarily, if A is a nonzero $1 \times n$ matrix over R and $d = \gcd(A)$, then there exists an invertible matrix V over R such that

$$AV = \begin{bmatrix} d & 0 & \cdots & 0 \end{bmatrix},$$

where V is the transpose of product of some elementary row operation matrices over R, i.e. V is a product of transpose of some elementary row operation matrices over R, and hence, a product of some elementary column operation matrices over R.

Input: An $m \times 1$ matrix A over R, where at least one entry is nonzero

Output: An $m \times 1$ matrix over R, where the first entry equals $\gcd(A)$ and other entries are zero

IF $R = \mathbb{Z}$ THEN

$k \leftarrow \min\left\{i \,:\, |a_{i1}| = \min\left\{|a_{i1}| \,:\, a_{i1} \neq 0,\ 1 \leq i \leq m\right\},\ 1 \leq i \leq m\right\}$

IF $R = \mathbb{F}[x]$ THEN

$k \leftarrow \min\left\{i \,:\, \deg\left(a_{i1}\right) = \min\left\{\deg\left(a_{i1}\right) \,:\, a_{i1} \neq 0,\ 1 \leq i \leq m\right\},\ 1 \leq i \leq m\right\}$

IF $k \neq 1$ THEN

Swap rows 1 and k

$i \leftarrow 2$

WHILE $i \leq m$ DO

IF $a_{i1} \neq 0$ THEN

Obtain q such that $a_{i1} = a_{11}q + r$ where $r = 0$ or $\phi(r) < \phi(a_{11})$

Add $-q$ times row 1 to row i

$i \leftarrow i + 1$

WHILE $(a_{i1} \neq 0$ for some $i = 2, \ldots, m)$ DO

IF $R = \mathbb{Z}$ THEN

$k \leftarrow \min\left\{i \,:\, |a_{i1}| = \min\left\{|a_{i1}| \,:\, a_{i1} \neq 0,\ 2 \leq i \leq m\right\},\ 2 \leq i \leq m\right\}$

IF $R = \mathbb{F}[x]$ THEN

$k \leftarrow \min\left\{i \,:\, \deg\left(a_{i1}\right) = \min\left\{\deg\left(a_{i1}\right) \,:\, a_{i1} \neq 0,\ 2 \leq i \leq m\right\},\ 2 \leq i \leq m\right\}$

Swap rows 1 and k

$i \leftarrow 2$

WHILE $i \leq m$ DO

IF $a_{i1} \neq 0$ THEN

Obtain q such that $a_{i1} = a_{11}q + r$ where $r = 0$ or $\phi(r) < \phi(a_{11})$

Add $-q$ times row 1 to row i

$i \leftarrow i + 1$

Algorithm 2.2: GCD of a finite subset of $\mathbb{Z}$ or $\mathbb{F}[x]$

Example 2.2.5. Let

$$A = \begin{bmatrix} 54 & -112 & -16 \end{bmatrix}^t$$

be a 3×1 matrix over $\mathbb{Z}$. Thus, we obtain the following:

$$\begin{bmatrix} 54 \\ -112 \\ -16 \end{bmatrix} \xrightarrow{\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}} \begin{bmatrix} -16 \\ -112 \\ 54 \end{bmatrix} \xrightarrow{\begin{bmatrix} 1 & 0 & 0 \\ -7 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}} \begin{bmatrix} -16 \\ 0 \\ 54 \end{bmatrix} \xrightarrow{\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3 & 0 & 1 \end{bmatrix}} \begin{bmatrix} -16 \\ 0 \\ 6 \end{bmatrix}$$

$$\begin{bmatrix} -16 \\ 0 \\ 6 \end{bmatrix} \xrightarrow{\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}} \begin{bmatrix} 6 \\ 0 \\ -16 \end{bmatrix} \xrightarrow{\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3 & 0 & 1 \end{bmatrix}} \begin{bmatrix} 6 \\ 0 \\ 2 \end{bmatrix} \xrightarrow{\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}} \begin{bmatrix} 2 \\ 0 \\ 6 \end{bmatrix} \xrightarrow{\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -3 & 0 & 1 \end{bmatrix}} \begin{bmatrix} 2 \\ 0 \\ 0 \end{bmatrix}.$$

Setting

$$U := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -3 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ -7 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 3 & 0 & 10 \\ 0 & 1 & -7 \\ -8 & 0 & -27 \end{bmatrix},$$

it follows that $UA = \begin{bmatrix} 2 & 0 & 0 \end{bmatrix}^t$. In other words, $\gcd(54, -112, -16) = 2$.

Example 2.2.6. Let

$$A = \begin{bmatrix} x^4-x^3-x^2+1 & x^2+x-2 & x^3-1 \end{bmatrix}^t$$

be a 3×1 matrix over $\mathbb{Q}[x]$, where $\mathbb{Q}$ is the field of rational numbers. Thus, we obtain the following:

$$\begin{bmatrix} x^4-x^3-x^2+1 \\ x^2+x-2 \\ x^3-1 \end{bmatrix} \xrightarrow{\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}} \begin{bmatrix} x^2+x-2 \\ x^4-x^3-x^2+1 \\ x^3-1 \end{bmatrix} \xrightarrow{\begin{bmatrix} 1 & 0 & 0 \\ -(x^2-2x+3) & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}} \begin{bmatrix} x^2+x-2 \\ -7x+7 \\ x^3-1 \end{bmatrix}$$

$$\begin{bmatrix} x^2+x-2 \\ -7x+7 \\ x^3-1 \end{bmatrix} \xrightarrow{\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -(x-1) & 0 & 1 \end{bmatrix}} \begin{bmatrix} x^2+x-2 \\ -7x+7 \\ 3x-3 \end{bmatrix} \xrightarrow{\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}} \begin{bmatrix} -7x+7 \\ x^2+x-2 \\ 3x-3 \end{bmatrix}$$

$$\begin{bmatrix} -7x+7 \\ x^2+x-2 \\ 3x-3 \end{bmatrix} \xrightarrow{\begin{bmatrix} 1 & 0 & 0 \\ \frac{1}{7}x+\frac{2}{7} & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}} \begin{bmatrix} -7x+7 \\ 0 \\ 3x-3 \end{bmatrix} \xrightarrow{\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \frac{3}{7} & 0 & 1 \end{bmatrix}} \begin{bmatrix} -7x+7 \\ 0 \\ 0 \end{bmatrix}$$

Setting

$$U := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \frac{3}{7} & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ \frac{1}{7}x+\frac{2}{7} & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -(x-1) & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ -(x^2-2x+3) & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & -(x^2-2x+3) & 0 \\ \frac{1}{7}x+\frac{2}{7} & -(\frac{1}{7}x^3-\frac{1}{7}x-\frac{1}{7}) & 0 \\ \frac{3}{7} & -(\frac{3}{7}x^2+\frac{1}{7}x+\frac{2}{7}) & 1 \end{bmatrix},$$

it follows that $UA = \begin{bmatrix} -7(x-1) & 0 & 0 \end{bmatrix}^t$. In other words,

$$\gcd(x^4-x^3-x^2+1,\, x^2+x-2,\, x^3-1) = x-1.$$

Remark 2.2.7. The results of this subsection generalize to any Euclidean domain.

2.3 Hermite normal form of a matrix over $\mathbb{Z}$

If a matrix is defined over a field, this matrix can be reduced to its row canonical form by performing some (finite) sequence of elementary row operations. In this section, an analogue of this reduction (when such matrix is defined over the ring of integers) will be briefly discussed, and this analogue is called Hermite normal form. Lemma 2.2.3 plays a major role in the computation of this Hermite normal form.

Definition 2.3.1. [4, p. 646] Let $H = (h_{ij})$ be an $m \times n$ matrix over $\mathbb{Z}$. Then H is in **Hermite normal form** if there exists a non-negative integer $r \leq m$ and positive integers $j_1, \ldots, j_r$ with $1 \leq j_1 < j_2 < \cdots j_r \leq n$ satisfying the following conditions:

(1) $h_{ij} = 0$ for $1 \leq i \leq r$ and $1 \leq j < j_i$, and also $h_{ij_i} \geq 1$ for $1 \leq i \leq r$, i.e. each leading entry (the first nonzero entry of a nonzero row) of H is positive.

(2) $0 \leq h_{kj_i} < h_{ij_i}$ for $1 \leq i \leq r$ and $1 \leq k < i$, i.e. each entry above a leading entry is non-negative and strictly less than the pivot element.

(3) $h_{ij} = 0$ for $r+1 \leq i \leq m$ and $1 \leq j \leq n$, i.e. the last $m-r$ rows of H are equal to zero.

The following result will only be stated without proof. A very similar result over $\mathbb{F}[x]$ will be stated in the next section, and there a proof will be given.

Theorem 2.3.2. *Let A be an $m \times n$ matrix over $\mathbb{Z}$. Then there exists a unique $m \times n$ matrix H over $\mathbb{Z}$ in Hermite normal form such that $UA = H$ for some $m \times m$ invertible matrix U over $\mathbb{Z}$. U being invertible over $\mathbb{Z}$ means U has integer entries and* $\det U = \pm 1$.

Proof. Very similar to proof of Theorem 2.4.2. Algorithm 2.3 is a constructive version of this proof. □

Definition 2.3.3. Let A be an $m \times n$ matrix over $\mathbb{Z}$. The $m \times n$ matrix H over $\mathbb{Z}$ in the theorem above is called the **Hermite normal form of A.**

Example 2.3.4. Let

$$A = \begin{bmatrix} 2 & 6 & 9 \\ -2 & 0 & 4 \\ 2 & 1 & -1 \end{bmatrix}$$

be a 3×3 matrix over $\mathbb{Z}$. The matrix A can be reduced to Hermite normal form by the following sequence of row operations defined over $\mathbb{Z}$.

$$\begin{bmatrix} 2 & 6 & 9 \\ -2 & 0 & 4 \\ 2 & 1 & -1 \end{bmatrix} \xrightarrow{U_1=\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}} \begin{bmatrix} 2 & 6 & 9 \\ 0 & 6 & 13 \\ 2 & 1 & -1 \end{bmatrix} \xrightarrow{U_2=\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix}} \begin{bmatrix} 2 & 6 & 9 \\ 0 & 6 & 13 \\ 0 & -5 & -10 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 6 & 9 \\ 0 & 6 & 13 \\ 0 & -5 & -10 \end{bmatrix} \xrightarrow{U_3=\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}} \begin{bmatrix} 2 & 6 & 9 \\ 0 & -5 & -10 \\ 0 & 6 & 13 \end{bmatrix} \xrightarrow{U_4=\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}} \begin{bmatrix} 2 & 6 & 9 \\ 0 & -5 & -10 \\ 0 & 1 & 3 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 6 & 9 \\ 0 & -5 & -10 \\ 0 & 1 & 3 \end{bmatrix} \xrightarrow{U_5=\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}} \begin{bmatrix} 2 & 6 & 9 \\ 0 & 1 & 3 \\ 0 & -5 & -10 \end{bmatrix} \xrightarrow{U_6=\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 5 & 1 \end{bmatrix}} \begin{bmatrix} 2 & 6 & 9 \\ 0 & 1 & 3 \\ 0 & 0 & 5 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 6 & 9 \\ 0 & 1 & 3 \\ 0 & 0 & 5 \end{bmatrix} \xrightarrow{U_7=\begin{bmatrix} 1 & -6 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}} \begin{bmatrix} 2 & 0 & -9 \\ 0 & 1 & 3 \\ 0 & 0 & 5 \end{bmatrix} \xrightarrow{U_8=\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}} \begin{bmatrix} 2 & 0 & 1 \\ 0 & 1 & 3 \\ 0 & 0 & 5 \end{bmatrix}$$

Setting

$$U := U_8U_7U_6U_5U_4U_3U_2U_1 = \begin{bmatrix} -1 & 4 & 6 \\ 0 & 1 & 1 \\ -1 & 5 & 6 \end{bmatrix} \quad \text{and} \quad H := \begin{bmatrix} 2 & 0 & 1 \\ 0 & 1 & 3 \\ 0 & 0 & 5 \end{bmatrix},$$

it follows that $UA = H$. In other words, the matrix H is the Hermite normal form of A.

2.4 Hermite normal form of a matrix over $\mathbb{F}[x]$

In this section, an Hermite normal form of matrices over the ring of polynomials $\mathbb{F}[x]$ in one indeterminate with coefficients in the field $\mathbb{F}$, will be discussed. The following definition is basically the same as Definition 2.3.1, except that entries of matrices are now from the ring of polynomials $\mathbb{F}[x]$ in one indeterminate x; thus the need for little adjustment in the definition.

Definition 2.4.1. Let $H = (h_{ij})$ be an $m \times n$ matrix over $\mathbb{F}[x]$. Then H is in **Hermite normal form** if there exists a non-negative integer $r \leq m$ and positive integers $j_1, \ldots, j_r$ with $1 \leq j_1 < j_2 < \cdots j_r \leq n$ satisfying the following conditions:
(1) $h_{ij} = 0$ for $1 \leq i \leq r$ and $1 \leq j < j_i$.
(2) h_{ij_i} is monic ($\mathrm{LC}\,(h_{ij_i}) = 1$) for $1 \leq i \leq r$.
(3) $h_{kj_i} = 0$ or $\deg\left(h_{kj_i}\right) < \deg\left(h_{ij_i}\right)$ for $1 \leq i \leq r$ and $1 \leq k < i$.
(4) $h_{ij} = 0$ for $r + 1 \leq i \leq m$ and $1 \leq j \leq n$.

Theorem 2.4.2. *Let A be an $m \times n$ matrix over $\mathbb{F}[x]$. Then there exists a unique $m \times n$ matrix H over $\mathbb{F}[x]$ in Hermite normal form such that $UA = H$ for some $m \times m$ invertible matrix U over $\mathbb{F}[x]$ (U being invertible implies $\det(U)$ is in $F\backslash\{0\}$).*

Proof. Only proof of the existence part of this theorem will be shown. The uniqueness part is proved in Adkins & Weintraub [1] (Theorem 5.2.13). The existence part of the theorem

will be shown by induction on the number of rows, m, of matrix A. To this end, let $T(m)$ be the statement that for every $m \times n$ (n being arbitrary) matrix A over $\mathbb{F}[x]$, there exists an $m \times n$ matrix H over $\mathbb{F}[x]$ in Hermite normal form such that $UA = H$ for some $m \times m$ invertible matrix U over $\mathbb{F}[x]$. For $m = 1$, let

$$A = \begin{bmatrix} 0 & 0 & \cdots & 0 & a_{1n_1} & a_{1n_2} & \cdots & a_{1n} \end{bmatrix}$$

be a $1 \times n$ matrix over $\mathbb{F}[x]$, where a_{1n_1} is the first nonzero entry (from left, so $1 \leq n_i \leq n$) in A. If a_{1n_1} is monic, then A is already in Hermite normal form, i.e. $UA = H$ where $U = I_1$, the 1×1 identity matrix and $H = A$. Otherwise,

$$H = \left[0, 0, \ldots, 0, \frac{1}{\mathrm{LC}\left(a_{1n_1}\right)} a_{1n_1}, \frac{1}{\mathrm{LC}\left(a_{1n_1}\right)} a_{1n_2}, \ldots, \frac{1}{\mathrm{LC}\left(a_{1n_1}\right)} a_{1n}\right] = UA,$$

where $U = \left[\frac{1}{\mathrm{LC}\left(a_{1n_1}\right)}\right]$. Hence, $T(1)$ is true. Now, suppose that $T(m-1)$ is true for $m > 2$. Let

$$A = \begin{bmatrix} 0 & \cdots & 0 & a_{1n_1} & a_{1n_2} & \cdots & a_{1n} \\ 0 & \cdots & 0 & a_{2n_1} & a_{2n_2} & \cdots & a_{2n} \\ 0 & \cdots & 0 & a_{3n_1} & a_{3n_2} & \cdots & a_{3n} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & a_{mn_1} & a_{mn_2} & \cdots & a_{mn} \end{bmatrix}$$

be any $m \times n$ matrix over $\mathbb{F}[x]$; assuming n_1 ($1 \leq n_1 \leq n$) is the smallest integer such that column n_1 of A is nonzero and a_{1n_1} is a nonzero entry with least degree in column n_1. By Lemma 2.2.3, if $d = \gcd\left(\{a_{in_1} : 1 \leq i \leq m\}\right)$, then there exists an invertible matrix U_1 over $\mathbb{F}[x]$ such that

$$U_1 A = A_1 = \begin{bmatrix} 0 & \cdots & 0 & d & * & \cdots & * \\ 0 & \cdots & 0 & 0 & * & \cdots & * \\ 0 & \cdots & 0 & 0 & * & \cdots & * \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & * & \cdots & * \end{bmatrix} = \begin{bmatrix} 0 & \cdots & 0 & d & * & \cdots & * \\ 0 & \cdots & 0 & 0 & & & \\ 0 & \cdots & 0 & 0 & & & \\ \vdots & \ddots & \vdots & \vdots & & B_1 & \\ 0 & \cdots & 0 & 0 & & & \end{bmatrix}.$$

The submatrix B_1 in A_1 is an $(m-1) \times (n-1)$ matrix over $\mathbb{F}[x]$ and so by the induction hypothesis, there exists an $(m-1) \times (n-1)$ matrix H' over $\mathbb{F}[x]$ in Hermite normal form such that $V'B_1 = H'$, for some $(m-1) \times (m-1)$ invertible matrix V' over $\mathbb{F}[x]$; which can be obtained from product of some elementary row operation matrices. That H' is in Hermite normal form implies by definition that there exists a non-negative integer r ($r \leq m-1$) and

positive integers $j_1, j_2, \ldots, j_r$ with $n_2 \leq j_1 < j_2 \cdots < j_r \leq n$ such that the conditions (1) - (4) of Definition 2.4.1 are satisfied. Setting

$$U_2 := \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & V' & \\ 0 & & & \end{bmatrix},$$

then the matrix

$$U_2 A_1 = A_2 = \begin{bmatrix} 0 & \cdots & 0 & d & b_{1n_2} & \cdots & b_{1n} \\ 0 & \cdots & 0 & 0 & & & \\ 0 & \cdots & 0 & 0 & & & \\ \vdots & \ddots & \vdots & \vdots & & H' & \\ 0 & \cdots & 0 & 0 & & & \end{bmatrix}$$

whose row indices are 1 more than row indices of H', satisfies all the conditions of Definition 2.4.1, except that the entries $b_{1j_1}, b_{1j_2}, \ldots, b_{1j_r}$ of matrix A_2 may not be reduced respectively with respect to entries $h'_{1j_1}, h'_{1j_2}, \ldots, h'_{1j_r}$ of matrix H'. From division algorithm, since each h'_{ij_i} $(1 \leq i \leq r)$ is nonzero, there exists unique q_{j_i} and r_{j_i} in $\mathbb{F}[x]$ such that $b_{1j_i} = q_{j_i} h'_{ij_i} + r_{j_i}$, i.e. $r_{j_i} = -q_{j_i} h'_{ij_i} + b_{1j_i}$. Therefore, for $1 \leq i \leq r$, multiplying row $i+1$ of matrices A_2 by $-q_{j_i}$ and then adding the result to row 1 of A_2, we finally obtain matrix H, in Hermite normal form and a matrix U_3 such that $U_3 A_2 = H$. Taking matrix U as the product of (invertible) matrices U_3, U_2 and U_1, i.e. $U = U_3 U_2 U_1$, then $UA = H$. Algorithm 2.3 is a constructive version of this proof. □

Definition 2.4.3. Let A be an $m \times n$ matrix over $\mathbb{F}[x]$. The $m \times n$ matrix H over $\mathbb{F}[x]$ in the theorem above is called the **Hermite normal form of** A**.**

Example 2.4.4. Let

$$A = \begin{bmatrix} x^2 & x & x \\ x^3 - 2x^2 & x^2 - x & x^2 - 2x \\ 2x^3 + x - 1 & x^2 & 2x^2 \end{bmatrix}$$

be a 3×3 matrix over $\mathbb{Q}[x]$, where $\mathbb{Q}$ is the field of rational numbers. The matrix A can be reduced to Hermite normal form by the following sequence of row operations defined over $\mathbb{Q}[x]$.

Input: An $m \times n$ matrix A over R

Output: An $m \times n$ matrix H over R and an (invertible) $m \times m$ matrix U over R such that $UA = H$.

Initialization: $i \leftarrow 1$, $j \leftarrow 1$.

WHILE ($i \leq m$ AND $j \leq n$) DO

VCOL $\leftarrow \{a_{i'j} \,:\, i \leq i' \leq m\}$

IF ($a = 0$ for all $a \in$ VCOL) THEN

$j \leftarrow j + 1$

ELSE

pivot $\leftarrow (i, j)$

SMALLEST NONZERO ENTRY TO PIVOT

IF $R = \mathbb{Z}$ THEN

$k \leftarrow \min\left\{i' \,:\, |a_{i'j}| = \min\left\{|a_{i'j}| \,:\, a_{i'j} \neq 0,\ i \leq i' \leq m\right\},\ i \leq i' \leq m\right\}$

IF $R = \mathbb{F}[x]$ THEN

$k \leftarrow \min\left\{i' : \deg\left(a_{i'j}\right) = \min\left\{\deg\left(a_{i'j}\right) : a_{i'j} \neq 0,\, i \leq i' \leq m\right\},\, i \leq i' \leq m\right\}$

IF $k \neq 1$ THEN

Swap rows i and k

IF $R = \mathbb{Z}$ AND $a_{ij} < 0$ THEN

Multiply row i by -1

IF $R = \mathbb{F}[x]$ AND $\mathrm{LC}\left(a_{ij}\right) \neq 1$ THEN

Multiply row i by $\frac{1}{\mathrm{LC}(a_{ij})}$

REDUCTION OF ENTRIES BELOW PIVOT – ALGORITHM 2.2

$i' \leftarrow i + 1$

WHILE $i' \leq m$ DO

IF $a_{i'j} \neq 0$ THEN

Obtain q such that $a_{i'j} = a_{ij}q + r$ where $r = 0$ or $\phi(r) < \phi(a_{ij})$

Add $-q$ times row i to row i'

$i' \leftarrow i' + 1$

Algorithm 2.3: Hermite normal form of a matrix over $\mathbb{Z}$ or $\mathbb{F}[x]$

WHILE $(a_{i'j} \neq 0$ for some $i' = i+1, \ldots, m)$ DO

IF $R = \mathbb{Z}$ THEN

$k \leftarrow \min\left\{i' : |a_{i'j}| = \min\left\{|a_{i'j}| : a_{i'j} \neq 0,\ i{+}1 \leq i' \leq m\right\},\ i{+}1 \leq i' \leq m\right\}$

IF $R = \mathbb{F}[x]$ THEN

$k \leftarrow \min\left\{i' \,:\, \deg\left(a_{i'j}\right) = \min\left\{\deg\left(a_{i'j}\right) \,:\, a_{i'j} \neq 0,\ i{+}1 \leq i' \leq m\right\}\right.$
$\left. i{+}1 \leq i' \leq m\right\}$

Swap rows i and k if $i \neq k$

$i' \leftarrow i + 1$

WHILE $i' \leq m$ DO

IF $a_{i'j} \neq 0$ THEN

Obtain q such that $a_{i'j} = a_{ij}q + r$ where $r = 0$ or $\phi(r) < \phi(a_{ij})$

Add $-q$ times row i to row i'

$i' \leftarrow i' + 1$

REDUCTION OF ENTRIES ABOVE PIVOT

$i' \leftarrow 1$

WHILE $i' < i$ DO

IF $a_{i'j} \neq 0$ THEN

Obtain q such that $a_{i'j} = a_{ij}q + r$ where $r = 0$ or $\phi(r) < \phi(a_{ij})$

Add $-q$ times row i to row i'

$i' \leftarrow i' + 1$

$i \leftarrow i + 1$

$j \leftarrow j + 1$

Algorithm 2.3: Hermite normal form of a matrix over $\mathbb{Z}$ or $\mathbb{F}[x]$, continued

$$A = \begin{bmatrix} x^2 & x & x \\ x^3-2x^2 & x^2-x & x^2-2x \\ 2x^3+x-1 & x^2 & 2x^2 \end{bmatrix} \xrightarrow[U_1A=A_1]{U_1=\begin{bmatrix} 1 & 0 & 0 \\ -(x-2) & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}} A_1 = \begin{bmatrix} x^2 & x & x \\ 0 & x & 0 \\ 2x^3+x-1 & x^2 & 2x^2 \end{bmatrix}$$

$$A_1 = \begin{bmatrix} x^2 & x & x \\ 0 & x & 0 \\ 2x^3+x-1 & x^2 & 2x^2 \end{bmatrix} \xrightarrow[U_2A_1=A_2]{U_2=\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -2x & 0 & 1 \end{bmatrix}} A_2 = \begin{bmatrix} x^2 & x & x \\ 0 & x & 0 \\ x-1 & -x^2 & 0 \end{bmatrix} \xrightarrow[U_3A_2=A_3]{U_3=\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}} A_3 = \begin{bmatrix} x-1 & -x^2 & 0 \\ 0 & x & 0 \\ x^2 & x & x \end{bmatrix}$$

$$A_3 = \begin{bmatrix} x-1 & -x^2 & 0 \\ 0 & x & 0 \\ x^2 & x & x \end{bmatrix} \xrightarrow[U_4A_3=A_4]{U_4=\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -(x+1) & 0 & 1 \end{bmatrix}} A_4 = \begin{bmatrix} x-1 & -x^2 & 0 \\ 0 & x & 0 \\ 1 & x^3+x^2+x & x \end{bmatrix} \xrightarrow[U_5A_4=A_5]{U_5=\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}} A_5 = \begin{bmatrix} 1 & x^3+x^2+x & x \\ 0 & x & 0 \\ x-1 & -x^2 & 0 \end{bmatrix}$$

$$A_5 = \begin{bmatrix} 1 & x^3+x^2+x & x \\ 0 & x & 0 \\ x-1 & -x^2 & 0 \end{bmatrix} \xrightarrow[U_6A_5=A_6]{U_6=\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1-x & 0 & 1 \end{bmatrix}} A_6 = \begin{bmatrix} 1 & x^3+x^2+x & x \\ 0 & x & 0 \\ 0 & -x^4-x^2+x & -x^2+x \end{bmatrix}$$

$$A_6 = \begin{bmatrix} 1 & x^3+x^2+x & x \\ 0 & x & 0 \\ 0 & -x^4-x^2+x & -x^2+x \end{bmatrix} \xrightarrow[U_7A_6=A_7]{U_7=\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & x^3+x-1 & 1 \end{bmatrix}} A_7 = \begin{bmatrix} 1 & x^3+x^2+x & x \\ 0 & x & 0 \\ 0 & 0 & -x^2+x \end{bmatrix}$$

$$A_7 = \begin{bmatrix} 1 & x^3+x^2+x & x \\ 0 & x & 0 \\ 0 & 0 & -x^2+x \end{bmatrix} \xrightarrow[U_8A_7=A_8]{U_8=\begin{bmatrix} 1 & -(x^2+x+1) & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}} A_8 = \begin{bmatrix} 1 & 0 & x \\ 0 & x & 0 \\ 0 & 0 & -x^2+x \end{bmatrix} \xrightarrow[U_9A_8=A_9]{U_9=\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}} A_9 = \begin{bmatrix} 1 & 0 & x \\ 0 & x & 0 \\ 0 & 0 & x^2-x \end{bmatrix}.$$

Setting

$$U := U_9U_8U_7U_6U_5U_4U_3U_2U_1 = \begin{bmatrix} x^3+x^2+x-1 & -x^2-x-1 & -x-1 \\ -x+2 & 1 & 0 \\ x^4+x^2-2x+1 & -x^3-x+1 & -x^2 \end{bmatrix} \quad \text{and} \quad H := A_4 = \begin{bmatrix} 1 & 0 & x \\ 0 & x & 0 \\ 0 & 0 & x^2-x \end{bmatrix},$$

it follows that $UA = H$. In other words, the matrix H is the Hermite normal form of A.

Chapter 3

Ranks of Matrices over Polynomial Rings

This chapter begins with a brief overview of the polynomial rings in more than one indeterminate over a field. Throughout this chapter, we write $X = \{x_1, \ldots, x_k\}$ $(k \geq 1)$ for a set of k indeterminates. Also, we write $\mathbb{F}$ to represent an arbitrary field, and $\mathbb{Z}_{\geq 0}$ for the set of non-negative integers.

A **monomial** in X is a product of the form $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_k^{\alpha_k}$, where $\alpha = (\alpha_1, \ldots, \alpha_k)$ belongs to $\mathbb{Z}_{\geq 0}^k$, and the **total degree** of x^α, denoted $|\alpha|$, equals $\alpha_1 + \cdots + \alpha_k$. A finite linear combination of monomials in X with coefficients in $\mathbb{F}$ is called a **polynomial** in X with coefficients in $\mathbb{F}$. The **set of all polynomials** in X with coefficients in $\mathbb{F}$ is denoted by $\mathbb{F}[X] = \mathbb{F}[x_1, \ldots, x_k]$. If an element in $\mathbb{F}[X]$ is chosen, say f, then f is of the form

$$f = \sum_\alpha a_\alpha x^\alpha$$

where the sum is over a finite number of k-tuples $\alpha = (\alpha_1, \ldots, \alpha_k) \in \mathbb{Z}_{\geq 0}^k$. In the above (finite) sum, each a_α is called the **coefficient** of corresponding monomial x^α. If in addition for each α that $a_\alpha \neq 0$, then $a_\alpha x^\alpha$ is called a **term** of f. The **total degree** of f, denoted $\deg(f)$, is the maximum $|\alpha|$ such that a_α is nonzero. For example, if $F = \mathbb{Q}$ (the field of rational numbers) and $X = \{x, y, z\}$, then

$$f = 4x^2 + 3xy + \frac{6}{7}x^2yz - \frac{9}{4}xyz - z + x^3z^4$$

is a polynomial in x, y, and z with coefficients in $\mathbb{Q}$. This polynomial has six terms and it has total degree seven. Defining addition on $\mathbb{F}[X]$ by

$$\sum_\alpha a_\alpha x^\alpha + \sum_\alpha b_\alpha x^\alpha = \sum_\alpha (a_\alpha + b_\alpha) x^\alpha,$$

and scalar multiplication on $\mathbb{F}[X]$ by

$$c \sum_\alpha a_\alpha x^\alpha = \sum_\alpha (ca_\alpha) x^\alpha,$$

for all $c \in \mathbb{F}$, then $\mathbb{F}[X]$ becomes a vector space over $\mathbb{F}$, with $\{x^\alpha : \alpha \in \mathbb{Z}^k_{\geq 0}\}$ (the set of all monomials in $\mathbb{F}[X]$) as a basis. In addition, defining multiplication on any two monomials of $\mathbb{F}[X]$ by $x^\alpha x^\beta = x^{\alpha+\beta}$, and thereafter extending this multiplication bilinearly to all of $\mathbb{F}[X]$, it follows that $\mathbb{F}[X]$ is a commutative associative unital ring. This ring is called the **polynomial ring** in k indeterminates $x_1, \ldots, x_k$ over $\mathbb{F}$. More studies relating to polynomial rings can be found in [12, ch. 5], [15, ch. 13] and [10, ch. 16].

In this chapter, the major references are Adkins and Weintraub [1, chs. 4 and 5], and Hoffman and Kunze [12, chs. 1, 2, 3 and 5].

3.1 Background to the problem

The purpose of this chapter is to extend some concepts from linear algebra over a field, to linear algebra over the polynomial ring $\mathbb{F}[x_1, \ldots, x_k]$. In particular, we want to be able to talk in a meaningful and well-defined way about the *rank* of an $m \times n$ matrix whose entries belong to $\mathbb{F}[x_1, \ldots, x_k]$.

Henceforth, unless explicitly stated otherwise, R will denote the polynomial ring $\mathbb{F}[X] = \mathbb{F}[x_1, \ldots, x_k]$, where $\mathbb{F}$ is a field. This field $\mathbb{F}$ can be field of any characteristic; however, for the purpose of computations, we will always use a field of characteristic zero. In addition, the field $\mathbb{F}$ needs not to be algebraically closed.

3.1.1 Equivalent definitions of the rank of matrices over a field

For an arbitrary matrix A over a field, the rank of A can be defined in a number of different ways. It is a basic theorem in linear algebra over a field that these definitions are actually equivalent. Thus, the rank of A will be denoted by $\text{rank}\,(A)$.

Let V be a vector space over the field $\mathbb{F}$. This vector space V has a **basis**, which is a spanning set of linearly independent vectors in V. All bases of a vector space have the same cardinality; this cardinality is called the **dimension** of V, denoted $\dim(V)$. If the cardinality is finite, then V is a **finite dimensional** vector space, and if the cardinality is infinite, then V is **infinite dimensional**. As an example, $\mathbb{F}^n$ is a finite dimensional vector space – one of its bases is the **standard (ordered) basis** $\{e_1, \ldots, e_n\}$, where e_i is the element (or vector)

in $\mathbb{F}^n$ with 1 in its i-th position and 0 elsewhere. An element in $\mathbb{F}^n$ may be regarded as either a row vector or a column vector, depending on the context.

Let A be an $m \times n$ matrix over the field $\mathbb{F}$, and let $A_1, \ldots, A_m \in \mathbb{F}^n$ stand for the rows of A, where

$$A_i = [A_{i1}, \ldots, A_{in}], \quad 1 \leq i \leq m.$$

In other words, each row of A is an element (or vector) in the vector space $\mathbb{F}^n$. The subspace of $\mathbb{F}^n$ spanned by $A_1, \ldots, A_m$, the rows of A, is called the **row space** of A. This subspace has a basis and the cardinality of this basis is called the **row rank** of A. In other words, the row rank of A is the dimension of the row space of A. The **column rank** of matrix A can be defined in a similar way, and it is also the row rank of A^t.

The rank of matrix A can also be defined using the concept of linear transformations. If U and V are vector spaces over the field $\mathbb{F}$, a **linear transformation from U to V** is a map $T : U \to V$ satisfying $T(cu_1 + u_2) = cT(u_1) + T(u_2)$ for all $u_1, u_2 \in U$ and all scalars $c \in \mathbb{F}$. The **null space** of T consists of all vectors u in U such that $T(u) = 0 \in V$, and it is a subspace of U. The **image** (or **range**) of T consists of all $T(u) \in V$ for $u \in U$; it is a subspace of V. The **rank** of T is the dimension of the image of T and the **nullity** of T is the dimension of the null space of T. In fact, if U is finite dimensional, then the sum of the rank of T, $\text{rank}\,(T)$ and the nullity of T, $\text{nullity}\,(T)$ equals the dimension of U, $\dim(U)$ i.e.

$$\text{rank}\,(T) + \text{nullity}\,(T) = \dim(U) \qquad \text{(Rank – Nullity Theorem)}.$$

If both U and V are finite dimensional with an ordered basis defined for each of them, then the linear transformation T can be represented with an $m \times n$ matrix $A = (a_{ij})$ over the field $\mathbb{F}$, where a_{ij} is the i-th coordinate, relative to the ordered basis of V, of image of the j-th basis vector of U. This matrix is called the **matrix representation** of T (or matrix of T) relative to the given ordered bases. On the other hand, if A is an $m \times n$ matrix over the field $\mathbb{F}$, then there is a linear transformation $T_A : \mathbb{F}^n \to \mathbb{F}^m$ defined by $T_A(X) = AX$, whose matrix representation is A with respect to the standard ordered bases of $\mathbb{F}^n$ and $\mathbb{F}^m$.

As a result of the above paragraph, it makes sense to talk about the transpose of a linear transformation T, denoted T^t, which is also a linear transformation, $T^t\colon (\mathbb{F}^m)^* \to (\mathbb{F}^n)^*$ defined by $\big(T^t g\big)(\alpha) = g\big(T(\alpha)\big)$, for every $g \in (\mathbb{F}^m)^*$ and $\alpha \in \mathbb{F}^n$. We note that for all k, $\big(\mathbb{F}^k\big)^*$ is a dual space of $\mathbb{F}^k$, and hence $\dim\Big(\big(\mathbb{F}^k\big)^*\Big) = \dim\big(\mathbb{F}^k\big)$ (Theorem 3.2.5 in [12]), i.e.

$\left(\mathbb{F}^k\right)^* \cong \mathbb{F}^k$. The matrix representing T^t (with respect to the standard ordered bases) is just the transpose of the matrix representing T. In fact, the rank of the linear transformation T, $\text{rank}\,(T)$ and the rank of its transpose, $\text{rank}\,(T^t)$ are equal, i.e. $\text{rank}\,(T) = \text{rank}\,(T^t)$. Given any $m \times n$ matrix over the field $\mathbb{F}$, the fact just mentioned is equivalent to the statement that the row rank of A equals the column rank of A. For if $T_A : \mathbb{F}^n \to \mathbb{F}^m$ is a linear transformation defined by $T_A(X) = AX$ for all $X = [x_1, \ldots, x_n]$ in $\mathbb{F}^n$, then the matrix representing T_A relative to the standard ordered bases for $\mathbb{F}^n$ and $\mathbb{F}^m$ is A. The rank of T, by definition, is the dimension of the image of T, which is the dimension of the column space of A, i.e. the column rank of A equals the rank of T. Similarly, for the transpose T^t of the transformation T, the rank of T^t is the dimension of the image of T^t, which is the dimension of the column space of the matrix A^t, since A^t is the matrix representing T^t. In other words, the rank of T^t equals the dimension of the row space of the matrix A (since columns of A^t are actually rows of A) i.e. the row rank of A equals the rank of T^t. Hence,

$$\text{column rank}\,(A) = \text{rank}\,(T), \qquad \text{row rank}\,(A) = \text{rank}\,(T^t),$$

and therefore

$$\text{column rank}\,(A) = \text{row rank}\,(A) \quad \text{if and only if} \quad \text{rank}\,(T) = \text{rank}\,(T^t).$$

Furthermore, in order to find the rank of an arbitrary matrix A over the field $\mathbb{F}$, this matrix can be reduced to a simpler form called **reduced row (resp. column) echelon form**, also called the **row (resp. column) canonical form**, by a sequence of elementary row (resp. column) operations. The row rank of A is the number of nonzero rows in the reduced row-echelon form of A, and the column rank of A is the number of nonzero rows in the reduced column-echelon form of A. From the above paragraph, the row rank of A equals the column rank of A, and thus the rank of A is just the number of nonzero rows (resp. columns) in the row (resp. column) reduced echelon form of A.

The concept of rank of a matrix over the field $\mathbb{F}$ can also be understood from the perspective of orthogonal complements of subspaces. Let U be an arbitrary subspace of $\mathbb{F}^n$. The orthogonal complement of U, denoted $U^\perp$ is the set

$$U^\perp = \{v \in \mathbb{F}^n \,:\, u \cdot v = 0 \text{ for all } u \in U\},$$

where $u \cdot v = \sum_{i=1}^n u_i v_i$ is the standard Euclidean dot product of two vectors u and v in $\mathbb{F}^n$. For any subspace U of $\mathbb{F}^n$, the intersection of U with its orthogonal complement $U^\perp$ is

the zero subspace denoted 0, and so the sum $U + U^{\perp}$ is direct; this is called the **internal direct sum** and denoted $U \oplus U^{\perp}$. In fact, the internal direct sum of U and $U^{\perp}$ equals $\mathbb{F}^n$, i.e. $U \oplus U^{\perp} = \mathbb{F}^n$. Now, let A be an $m \times n$ matrix over the field $\mathbb{F}$. The row space of A is a subspace of $\mathbb{F}^n$. Writing $X := (X_1, \ldots, X_n) \in \mathbb{F}^n$ for the components of X, then

$$
\begin{aligned}
X \in \big(\text{rowspace}(A)\big)^{\perp} &\iff X \cdot Y = 0 \text{ for all } Y \in \text{rowspace}(A) \\
&\iff X \cdot \sum_{i=1}^{m} c_i A_i = 0, \text{ for all } c_1, \ldots, c_m \in \mathbb{F} \\
&\iff \sum_{i=1}^{m} c_i (X \cdot A_i) = 0, \text{ for all } c_1, \ldots, c_m \in \mathbb{F} \\
&\iff X \cdot A_i = 0, \ \ i = 1, \ldots, m \\
&\iff (X_1, \ldots, X_n) \cdot (A_{i1}, \ldots, A_{in}) = 0, \ \ i = 1, \ldots, m \\
&\iff \sum_{j=1}^{n} X_j A_{ij} = 0, \ \ i = 1, \ldots, m \\
&\iff \sum_{j=1}^{n} A_{ij} X_j = 0, \ \ i = 1, \ldots, m \\
&\iff AX = 0 \in \mathbb{F}^m \\
&\iff X \in \text{nullspace}(A),
\end{aligned}
$$

where nullspace(A) is the null space of A. Thus, the internal direct sum rowspace$(A) \oplus$ nullspace$(A) = \mathbb{F}^n$ is obtained, where nullspace$(A) = \big(\text{rowspace}(A)\big)^{\perp}$. Consequently, the rank of an $m \times n$ matrix A over the field $\mathbb{F}$ equals $n -$ nullity (A), where nullity (A) is the dimension of the null space of A.

3.1.2 Generic rank of matrices over polynomial rings

The definitions of rank that have been considered so far depend on the fact that any vector space (or subspace) has a well-defined dimension. Of much interest to us is computing some well-defined *rank* (if possible) of any arbitrary matrix over the polynomial ring $R = \mathbb{F}[x_1, \ldots, x_k]$. There are many ways to define what we mean by the *rank* of such a matrix, but in general they give different answers. The simplest way to define the rank of a matrix over such a ring R is to pass to its field of fractions, namely the field of rational

functions $\mathbb{F}(x_1, \ldots, x_k)$, consisting of all elements of the form f/g where $f, g \in R$. Since every polynomial is a rational function, by taking $g = 1$, a matrix over R may be regarded as a matrix over the field $\mathbb{F}(x_1, \ldots, x_k)$. Since $\mathbb{F}(x_1, \ldots, x_k)$ is a field, all the results of elementary linear algebra apply, and so we may compute the (unique and well-defined) reduced row echelon form of any matrix with entries in $\mathbb{F}(x_1, \ldots, x_k)$; the number of nonzero rows in the resulting matrix is called the **generic rank** of the original polynomial matrix.

The problem with the above approach is that in general the entries of the row canonical form will have nontrivial denominators. We may take two different points of view regarding the variables in $\mathbb{F}[X]$: either they are indeterminates with no value, or we may assign to them values in $\mathbb{F}$. If we assign values in $\mathbb{F}$ to the variables in $\mathbb{F}[X]$ which make one or more of those denominators equal to 0, we will obtain an undefined result. For example, consider below a 3×4 matrix A over the ring of polynomials $\mathbb{Q}[a, b]$ (where $\mathbb{Q}$ is the field of rational numbers), with its reduced row echelon form, $\mathrm{RREF}(A)$ over the field of rational functions $\mathbb{Q}(a, b)$:

$$A = \begin{bmatrix} b & 1 & 1 & a \\ -b^2 & -b & a-b & b-ab \\ 0 & 0 & a & b \end{bmatrix}, \qquad \mathrm{RREF}(A) = \begin{bmatrix} 1 & \frac{1}{b} & 0 & \frac{a^2-b}{ab} \\ 0 & 0 & 1 & \frac{b}{a} \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

The generic rank of this matrix is 2, since there are two nonzero rows in $\mathrm{RREF}(A)$. From the row canonical form, neither of the variables x and y can be zero as that will give an undefined result. For any other values of the variables, the rank of the matrix obtained by substituting these values into the original matrix will equal the generic rank. In general, for any values of the variables, the rank of the (scalar) matrix obtained by substituting these values into the original matrix will be less than or equal to the generic rank. In particular, substituting 0 for both x and y in the original matrix, it is easy to see that the rank of the (scalar) matrix obtained after this substitution is 1, which is less than 2, the generic rank. In general, values of the variables $x_1, \ldots, x_k$ that give a rank less than or exactly equal to the generic rank, after substitution into the original matrix, can be determined without having to pass to the field of fractions, i.e. without having to do divisions. The theory of determinantal ideals helps in determining such values.

3.2 Determinantal rank

In this section, we consider another approach of possibly defining the rank of a polynomial matrix. The determinant, which is well-defined for square matrices over any commutative ring, plays a major role in this section. So there is a need to first discuss briefly the concept *determinant*, as a function over some set of square matrices.

3.2.1 Determinants

In this section, the definition of a determinant function will be given, and also, some elementary results will be stated with proofs. Though more results on determinant function can be found in [1] and [12], only those results that fit in into the purpose of this thesis are considered. Throughout this section, R will represent a commutative ring with identity. For an $n \times n$ matrix A over R, here in this section, we will write $\text{row}(i, A)$ to represent the i-th row of A. In addition, for $1 \leq i \leq n$, if $A_i = \text{row}(i, A)$, then we will write $(A_1, \ldots, A_n)$ to represent matrix A, i.e.

$$A = \begin{pmatrix} A_1 \\ \vdots \\ A_n \end{pmatrix} = (A_1, \ldots, A_n).$$

Definition 3.2.1. Let $M_n(R)$ $(n \geq 1)$ be the set of all $n \times n$ (square) matrix over R. A function $D : M_n(R) \to R$ is called a **determinant function** if the following three properties are satisfied:

(a) D is ***n*-linear** on rows of matrices in $M_n(R)$. In other words, for any three $n \times n$ matrices A, B and C that differ only in their i-th rows, i.e. $A_j = B_j = C_j$ where $1 \leq j \neq i \leq n$ and $1 \leq i \leq n$, if we set $D(A) = D(A_1, \ldots, A_i, \ldots, A_n)$, $D(B) = D(A_1, \ldots, B_i, \ldots, A_n)$ and $D(C) = D(A_1, \ldots, r\,A_i + B_i, \ldots, A_n)$, then $D(C) = r\,D(A) + D(B)$, i.e.

$$D(A_1, \ldots, rA_i + B_i, \ldots, A_n) = r\,D(A_1, \ldots, A_i, \ldots, A_n) + D(A_1, \ldots, B_i, \ldots, A_n),$$

for $r \in R$.

(b) D is alternating. That is, $D(A) = 0$ whenever two rows of A are equal.

(c) $D(I_n) = 1$, where I_n is the $n \times n$ identity matrix over R.

Lemma 3.2.2. *Let A be an $n \times n$ matrix over R, $D\colon M_n(R) \to R$ be a determinant function, and E be an elementary row operation matrix. For $1 \leq p \neq q \leq n$,*

1. *if E interchanges rows p and q of A, then $D(EA) = -D(A)$,*
2. *if E multiplies row p of A by a nonzero element $r \in R$, then $D(EA) = r\,D(A)$,*
3. *if E adds a multiple of row p of A to row q of A, then $D(EA) = D(A)$.*

Proof. The proof is as follows:

1. Let $A_i = \text{row}(i, A)$, $1 \leq i \leq n$. Suppose the p-th and q-th rows of A are A_p and A_q respectively. Setting $A = (A_1, \ldots, A_p, \ldots, A_q, \ldots, A_n)$, then
$$EA = (A_1, \ldots, A_q, \ldots, A_p, \ldots, A_n).$$
Let B be an $n \times n$ matrix over R which differ from A only in its p-th and q-th rows. If $\text{row}(p, B) = A_p + A_q = \text{row}(q, B)$, then by property (b) of Definition 3.2.1, $D(B) = 0$, reason being that D is a determinant function. Therefore, setting
$$B = (A_1, \ldots, A_p + A_q, \ldots, A_p + A_q, \ldots, A_n),$$
it follows from properties (a) and (b) of Definition 3.2.1 that
$$\begin{aligned}
0 &= D(B) \\
&= D(A_1, \ldots, A_p + A_q, \ldots, A_p + A_q, \ldots, A_n) \\
&= D(A_1, \ldots, A_p, \ldots, A_p + A_q, \ldots, A_n) + D(A_1, \ldots, A_q, \ldots, A_p + A_q, \ldots, A_n) \\
&= D(A_1, \ldots, A_p, \ldots, A_p, \ldots, A_n) + D(A_1, \ldots, A_p, \ldots, A_q, \ldots, A_n) \\
&\quad + D(A_1, \ldots, A_q, \ldots, A_p, \ldots, A_n) + D(A_1, \ldots, A_q, \ldots, A_q, \ldots, A_n) \\
&= 0 + D(A_1, \ldots, A_p, \ldots, A_q, \ldots, A_n) + D(A_1, \ldots, A_q, \ldots, A_p, \ldots, A_n) + 0 \\
&= D(A) + D(EA),
\end{aligned}$$
i.e. $D(EA) = -D(A)$, as required.
2. Here, setting $A = (A_1, \ldots, A_p, \ldots, A_n)$, then $EA = (A_1, \ldots, r\,A_p, \ldots, A_n)$. It therefore follows from only property (a) of Definition 3.2.1 that
$$D(EA) = D(A_1, \ldots, r\,A_p, \ldots, A_n) = r\,D(A_1, \ldots, A_p, \ldots, A_n) = rD(A),$$
i.e. $D(EA) = r\,D(A)$, as required.

3. Here, setting $A = (A_1, \ldots, A_p, \ldots, A_q, \ldots, A_n)$, then

$$EA = (A_1, \ldots, A_p, \ldots, r\,A_p + A_q, \ldots, A_n),$$

$r \in R$. It therefore follows from properties (a) and (b) of Definition 3.2.1 that

$$\begin{aligned} D(EA) &= D(A_1, \ldots, A_p, \ldots, r\,A_p + A_q, \ldots, A_n) \\ &= r\,D(A_1, \ldots, A_p, \ldots, A_p, \ldots, A_n) + D(A_1, \ldots, A_p, \ldots, A_q, \ldots, A_n) \\ &= r \cdot 0 + D(A_1, \ldots, A_p, \ldots, A_q, \ldots, A_n) \\ &= D(A), \end{aligned}$$

i.e. $D(EA) = D(A)$, as required.

This completes the proof. □

It has been shown that there is at least one determinant function on $M_n(R)$, the set of all $n \times n$ matrices over R (Section 2 in Chapter 5 of [12]). In fact, it was further shown that there is no more than one determinant function on $M_n(R)$ (Section 3 in Chapter 5 of [12]). In other words, the determinant function D on $M_n(R)$ exists and it is unique (another reference is [1], Theorem 2.8 in Chapter 4). Henceforth, we write **det** for the determinant function $D\colon M_n(R) \to R$.

3.2.2 Determinantal rank and determinantal ideals

In this subsection, a brief background and basic results on determinantal ranks and determinantal ideals in $R = \mathbb{F}[X] = \mathbb{F}[x_1, \ldots, x_k]$, will be given. At some point, the concept of determinantal ideals will be used to determine (without having to do division) the values of the variables $x_1, \ldots, x_k$, after substitution into an arbitrary matrix A over R, that will give a rank less than or equal to the generic rank of A. More study about determinantal ranks can be found in [1].

For a better understanding of this subsection, it is important to give some notations, just as in [1] (Chapter 4, Section 2). For positive integers r and m with $r \leq m$, let $\mathcal{C}(r, m)$ be a set of all *ordered* r-tuple $(i_i, \ldots, i_r)$, where $1 \leq i_1 < i_2 < \cdots i_r \leq m$, i.e.

$$\mathcal{C}(r, m) = \{\alpha = (i_1, \ldots, i_r) \,:\, 1 \leq i_1 < i_2 < \cdots < i_r \leq m\}\,.$$

The cardinality of $\mathcal{C}(r,m)$ is $|\mathcal{C}(r,m)| = \binom{m}{r}$. If $A = (a_{ij})$ is an $m \times n$ matrix over R, $\alpha \in \mathcal{C}(r,m)$ and $\beta \in \mathcal{C}(s,n)$, then $A[\alpha|\beta]$ will denote the $r \times s$ submatrix of A consisting of entries of A whose row index and column index are in α and β, respectively. For example, let $A = (a_{ij})$ be an $m \times n$ ($m \geq 5$ and $n \geq 5$) matrix over R, $\alpha = (3,5) \in \mathcal{C}(2,m)$ and $\beta = (1,4,n) \in \mathcal{C}(3,n)$. Then,

$$A[\alpha|\beta] = \begin{bmatrix} a_{31} & a_{34} & a_{3n} \\ a_{51} & a_{54} & a_{3n} \end{bmatrix}.$$

Definition 3.2.3. Let A be an $m \times n$ matrix over R and r be a positive integer with $r \leq \min\{m,n\}$. A $\boldsymbol{r \times r}$ **minor** of A is the determinant of any $r \times r$ submatrix of A.

Remark 3.2.4. Let A be a matrix over R. From the above definition, any $r \times r$ minor of A is an element of R. If we set

$$M_r(A) = \left\{ \det\left(A[\alpha|\beta]\right) \,:\, \alpha \in \mathcal{C}(r,m),\, \beta \in \mathcal{C}(r,n) \right\} \subseteq R,$$

then $M_r(A)$ is the set of all $r \times r$ minors of A.

Definition 3.2.5. [1, p. 205] Let A be an $m \times n$ matrix over R. The largest (positive) integer $r \leq \min\{m,n\}$ such that there is a nonzero $r \times r$ minor of A is called the **determinantal rank** of A, denoted D-rank(A).

Example 3.2.6. Let $R = \mathbb{Q}[a,b]$ and

$$A = \begin{bmatrix} b & 1 & 1 & a \\ -b^2 & -b & a-b & b-ab \\ 0 & 0 & a & b \end{bmatrix}$$

be a 3×4 matrix over R. The sets of all $r \times r$ ($r = 1,2,3$) minors of A are:

$$\begin{aligned} M_1(A) &= \left\{0,\, 1,\, a,\, b, -b,\, a-b,\, -b^2,\, b-ab\right\}, \\ M_2(A) &= \left\{0,\, a,\, b,\, b^2,\, -b^2,\, ab,\, -ab,\, b-a^2, -b^3,\, -ab^2,\, a^2b-b^2\right\}, \\ M_3(A) &= \{0\}. \end{aligned}$$

Therefore, the determinantal rank of A is D-rank$(A) = 2$.

Definition 3.2.7. Let A be an $m \times n$ matrix over R and r be a (positive) integer with $r \leq \min\{m, n\}$. The ideal in R generated by all $r \times r$ minors of A is called the ***r*-th determinantal ideal** of A, denoted $DI_r(A)$. In other words,

$$DI_r(A) = \big\langle M_r(A) \big\rangle \subseteq R,$$

where $M_r(A)$ is the set of all $r \times r$ minors of A. By convention, we set $DI_0(A) = R$ and $DI_r(A) = 0$, if $r > \min\{m, n\}$.

Example 3.2.8. Let $R = \mathbb{Q}[a, b]$ and

$$A = \begin{bmatrix} b & 1 & 1 & a \\ -b^2 & -b & a-b & b-ab \\ 0 & 0 & a & b \end{bmatrix}$$

be a 3×4 matrix over R, as in Example 3.2.6. The r-th ($r = 1, 2, 3$) determinantal ideals of A are:

$$\begin{aligned} DI_1(A) &= \big\langle \{0,\, 1,\, a,\, b, -b,\, a-b,\, -b^2,\, b-ab\} \big\rangle \;=\; \big\langle 1 \big\rangle = \; \mathbb{Q}[a, b], \\ DI_2(A) &= \big\langle \{0,\, a,\, b,\, b^2,\, -b^2,\, ab,\, -ab,\, b-a^2, -b^3,\, -ab^2,\, a^2b-b^2\} \big\rangle \;=\; \big\langle a,\, b \big\rangle, \\ DI_3(A) &= \big\langle \{0\} \big\rangle \;=\; \big\langle 0 \big\rangle. \end{aligned}$$

Definition 3.2.9. [7, p. 79] Let $I \subseteq R$ be an ideal. The set of points

$$\mathbb{V}\big(I\big) = \big\{(x_1, \ldots, x_k) \in \mathbb{F}^k \colon\; f(x_1, \ldots, x_k) = 0 \;\forall\; f \in I\big\}$$

is called the **zero set** of the ideal I.

Remark 3.2.10. Let A be an $m \times n$ matrix over $R = \mathbb{F}[x_1, \ldots, x_k]$, and r be a non-negative integer $\leq \min\{m, n\}$. Suppose $(a_1, \ldots, a_k) \in \mathbb{F}^k$ is a point in $\mathbb{V}\big(DI_{r+1}(A)\big) \backslash \mathbb{V}\big(DI_r(A)\big)$, and let B be an $m \times n$ matrix over $\mathbb{F}$, obtained by substituting the point $(a_1, \ldots, a_k)$ for $(x_1, \ldots, x_k)$ in A. Then we obtain the following:

$$\begin{aligned} & (a_1, \ldots, a_k) \in \mathbb{V}\big(DI_{r+1}(A)\big) \backslash \mathbb{V}\big(DI_r(A)\big) \\ \iff & (a_1, \ldots, a_k) \in \mathbb{V}\big(DI_{r+1}(A)\big) \;\text{ but }\; (a_1, \ldots, a_k) \notin \mathbb{V}\big(DI_r(A)\big) \\ \iff & f(a_1, \ldots, a_k) = 0 \;\forall\; f \in DI_{r+1}(A), \;\text{ but }\; \exists\; g \in DI_r(A) \;\text{ such that }\; g(a_1, \ldots, a_k) \neq 0 \\ \iff & DI_{r+1}(A)\Big|_{(x_1, \ldots, x_k) = (a_1, \ldots, a_k)} = \langle 0 \rangle, \quad \text{and} \quad DI_r(A)\Big|_{(x_1, \ldots, x_k) = (a_1, \ldots, a_k)} \neq \langle 0 \rangle \\ \iff & \operatorname{rank}(B) = r. \end{aligned}$$

From Definition 3.2.7, $DI_0(A) = \mathbb{F}[x_1, \ldots, x_k]$ and $DI_r(A) = 0$, if $r > \min\{m, n\}$, implying $\mathbb{V}\big(DI_0(A)\big) = \emptyset$ and $\mathbb{V}\big(DI_r(A)\big) = \mathbb{F}^k$, if $r > \min\{m, n\}$

Example 3.2.11. Let $R = \mathbb{Q}[a, b]$ and

$$A = \begin{bmatrix} b & 1 & 1 & a \\ -b^2 & -b & a-b & b-ab \\ 0 & 0 & a & b \end{bmatrix}$$

be a 3×4 matrix over R, as in Example 3.2.8. The zero sets of the r-th ($r = 1, 2, 3$) determinantal ideals of A are:

$$\begin{aligned} \mathbb{V}\big(DI_1(A)\big) &= \mathbb{V}\big(\langle 1 \rangle\big) = \mathbb{V}\big(\mathbb{Q}[a, b]\big) = \emptyset, \\ \mathbb{V}\big(DI_2(A)\big) &= \mathbb{V}\big(\langle a,\, b \rangle\big) = \{(0, 0)\}, \\ \mathbb{V}\big(DI_3(A)\big) &= \mathbb{V}\big(\langle 0 \rangle\big) = \mathbb{Q}^2. \end{aligned}$$

Therefore, by Remark 3.2.10, we obtain the following about the scalar matrices obtained after substituting the points in the zero sets above into A.

r	set of point(s) $(a, b) \in \mathbb{Q}^2$, after substitution into A, that correspond to rank r
0	$\mathbb{V}\big(DI_1(A)\big) \backslash \mathbb{V}\big(DI_0(A)\big) = \emptyset$
1	$\mathbb{V}\big(DI_2(A)\big) \backslash \mathbb{V}\big(DI_1(A)\big) = \{(0, 0)\}$
2	$\mathbb{V}\big(DI_3(A)\big) \backslash \mathbb{V}\big(DI_2(A)\big) = \{(a, b) : (a, b) \neq (0, 0)\}$.

Example 3.2.12. Let $R = \mathbb{Q}[a, b]$ and

$$A = \begin{bmatrix} b & a & 0 \\ b & 0 & 1 \\ b & 0 & a \end{bmatrix}$$

be a 3×3 matrix over R. The sets of all $r \times r$ ($r = 1, 2, 3$) minors of A are:

$$\begin{aligned} M_1(A) &= \{b,\, a,\, 0,\, 1\}, \\ M_2(A) &= \left\{-ab,\, b,\, a,\, ab,\, a^2,\, 0,\, ab-b\right\}, \\ M_3(A) &= \left\{-a^2b + ab\right\}. \end{aligned}$$

Therefore, D-rank$(A) = 3$. Furthermore, the r-th ($r = 1, 2, 3$) determinantal ideals of A are:

$$
\begin{aligned}
DI_1(A) &= \big\langle \{b,\, a,\, 0,\, 1\} \big\rangle = \big\langle 1 \big\rangle, \\
DI_2(A) &= \big\langle \big\{ -ab,\, b,\, a,\, ab,\, a^2,\, 0,\, ab-b \big\} \big\rangle = \big\langle a, b \big\rangle, \\
DI_3(A) &= \big\langle \big\{ -a^2b + ab \big\} \big\rangle = \big\langle a^2b - ab \big\rangle.
\end{aligned}
$$

In addition, the zero sets of the r-th ($r = 1, 2, 3$) determinantal ideals of A are:

$$
\begin{aligned}
\mathbb{V}\big(DI_1(A)\big) &= \mathbb{V}\big(\langle 1 \rangle\big) \;=\; \emptyset, \\
\mathbb{V}\big(DI_2(A)\big) &= \mathbb{V}\big(\langle a,\, b \rangle\big) \;=\; \{(0,0)\}, \\
\mathbb{V}\big(DI_3(A)\big) &= \mathbb{V}\big(\langle ab(a-1) \rangle\big) \;=\; \{(0,b),\, (a,0),\, (1,b) \,:\, a, b \in \mathbb{Q}\}.
\end{aligned}
$$

Hence, we obtain

r	set of point(s) $(a,b) \in \mathbb{Q}^2$, after substitution into A, that correspond to rank r
0	$\emptyset$
1	$\{(0,0)\}$
2	$\{(0,b),\, (a,0),\, (1,b) \,:\, a, b \in \mathbb{Q},\, (a,b) \neq (0,0)\}$
3	all $(a,b) \in \mathbb{Q}^2$ such that $(a,b) \notin \{(0,b),\, (a,0),\, (1,b)\}$

and this completes the example.

It will now be shown that the determinantal ideals are invariant (remain unchanged) under the (left) action of an elementary row operation on a matrix. But before then, an important property of elementary matrices will be stated with proof. Though the result is restricted to only elementary row operations, exactly same argument of the proof can be used if only elementary column operations are allowed, in lieu of the row operations.

Lemma 3.2.13. *Let A be an $m \times n$ matrix over R. If E is an arbitrary elementary row operation matrix on A, then the inverse of E exists and it is also an elementary row operation matrix.*

Proof. Let E^{-1} represent the inverse of an $m \times m$ elementary matrix $E = (e_{ij})$. First, assuming $1 \leq p < q \leq m$ and suppose E interchanges rows p and q of A. Then E has entries $e_{pq} = 1$, $e_{qp} = 1$, $e_{ii} = 1$, for $1 \leq i \leq m$, $i \neq p$ and $i \neq q$, and 0 elsewhere, i.e.

$$E = \begin{array}{c} \\ p \\ \\ q \\ \\ \end{array}\!\!\begin{array}{c} \begin{array}{ccccccc} & & & p & & q & \end{array} \\ \begin{bmatrix} 1 & \dots & 0 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & 1 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 1 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & 0 & \dots & 1 \end{bmatrix} \end{array}.$$

We claim that $E^{-1} = E$. In order to verify this claim, it suffices to show that $EE^{-1} = I_m$, the $m \times m$ identity matrix. In fact, if $EE^{-1} = (\epsilon_{ij})$, in order to show that $EE^{-1} = I_m$, we only need to show that the entries ϵ_{pp} and ϵ_{qq} in the matrix multiplication EE^{-1} are both 1. Using matrix multiplication formula,

$$\epsilon_{pp} = \sum_{k=1}^{m} e_{pk}e_{kp} = e_{pq}e_{qp} = 1, \quad \textit{and} \quad \epsilon_{qq} = \sum_{k=1}^{m} e_{qk}e_{kq} = e_{qp}e_{pq} = 1,$$

as expected. Second, suppose E multiplies row p of A by a nonzero element $u \in \mathbb{F}$. Then E has entries $e_{pp} = u$, $e_{ii} = 1$, for $1 \leq i \neq p \leq m$, and 0 elsewhere. We claim here that the inverse of E is a matrix with same entries as entries in E except that the entry in its row p and column p is now $\frac{1}{u}$. In other words, if

$$E = \begin{array}{c} \\ p \\ \\ \end{array}\!\!\begin{array}{c} \begin{array}{ccccc} & & p & & \end{array} \\ \begin{bmatrix} 1 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & u & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & 1 \end{bmatrix} \end{array}, \qquad \text{then} \qquad E^{-1} = \begin{array}{c} \\ p \\ \\ \end{array}\!\!\begin{array}{c} \begin{array}{ccccc} & & p & & \end{array} \\ \begin{bmatrix} 1 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & \frac{1}{u} & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & 1 \end{bmatrix} \end{array}.$$

This is true since the entry in row p and column p of the matrix multiplication EE^{-1} is $u \cdot \frac{1}{u} = 1$. Lastly, assuming $1 \leq p \neq q \leq m$, and suppose E adds a multiple, say $r \in R$ of row p of A to row q of A. If $p < q$ (resp. $p > q$), then E has entries $e_{qp} = r$, $e_{ii} = 1$, for $1 \leq i \leq m$, and 0 elsewhere. Here, the inverse of E is a matrix with same entries as entries in E except that the entry in its row q and column p is now $-r$. In other words, if

$$E = \begin{array}{c} \\ p \\ \\ q \\ \\ \end{array}\!\!\begin{array}{c} \begin{array}{ccccccc} & & & p & & q & \end{array} \\ \begin{bmatrix} 1 & \dots & 0 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 1 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & r & \dots & 1 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & 0 & \dots & 1 \end{bmatrix} \end{array}, \qquad (\text{resp.} \qquad E = \begin{array}{c} \\ q \\ \\ p \\ \\ \end{array}\!\!\begin{array}{c} \begin{array}{ccccccc} & & & q & & p & \end{array} \\ \begin{bmatrix} 1 & \dots & 0 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 1 & \dots & r & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & 1 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & 0 & \dots & 1 \end{bmatrix} \end{array}),$$

then

$$E^{-1} = \begin{array}{c} \\ p \\ \\ q \\ \\ \end{array}\!\!\begin{array}{c} \begin{array}{ccccccc} & & p & & q & & \end{array} \\ \begin{bmatrix} 1 & \dots & 0 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 1 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & -r & \dots & 1 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & 0 & \dots & 1 \end{bmatrix} \end{array}, \qquad \text{(resp.} \qquad E^{-1} = \begin{array}{c} \\ q \\ \\ p \\ \\ \end{array}\!\!\begin{array}{c} \begin{array}{ccccccc} & & q & & p & & \end{array} \\ \begin{bmatrix} 1 & \dots & 0 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 1 & \dots & -r & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & 1 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & 0 & \dots & 1 \end{bmatrix} \end{array}\text{).}$$

In order to verify that $EE^{-1} = I_m$, it suffices to show that the entry in row q and column p of the matrix multiplication EE^{-1} is 0. To this end, suppose $E^{-1} = (e'_{ij})$ and $EE^{-1} = (\epsilon_{ij})$. Using the matrix multiplication formula, we obtain

$$\epsilon_{qp} = \sum_{k=1}^{m} e_{qk}e'_{kp} = e_{qp}e'_{pp} + e_{qq}e'_{qp} = r - r = 0,$$

as expected. □

Proposition 3.2.14. *Let A be an $m \times n$ matrix over R, and E be an elementary row operation on A. Then for $r = 1, \dots, \min\{m, n\}$,*

$$DI_r(EA) = DI_r(A).$$

Proof. We follow the same argument in Lemma 11.2.1 of [16]. Let r $(1 \leq r \leq \min\{m, n\})$ be fixed. For a fixed element $\alpha = (i_1, \dots, i_r) \in \mathcal{C}(r, m)$, and arbitrary element $\beta \in \mathcal{C}(r, n)$, the matrix $A[\alpha|\beta]$ is an $r \times r$ submatrix of A, and so $\det\big(A[\alpha|\beta]\big)$ belongs to $DI_r(A)$. It will first be shown that $DI_r(EA) \subseteq DI_r(A)$ by considering the different effects of elementary row operations E on A. To this end, setting $B = EA$, $\det\big(B[\alpha|\beta]\big)$ belongs to $DI_r(EA)$, and if i_p and i_q are any row indices of A, then we obtain the following:

Case 1: Suppose E interchanges rows i_p and i_q of A.

(a) If $i_p,\ i_q \notin \{i_1, i_2, \dots, i_r\}$, then $\text{row}(i_p, A) = \text{row}(i_p, B)$ and $\text{row}(i_q, A) = \text{row}(i_q, B)$, and so

$$\det\big(B[\alpha|\beta]\big) = \det\big(A[\alpha|\beta]\big) \in DI_r(A).$$

(b) If $i_p,\ i_q \in \{i_1, i_2, \dots, i_r\}$, then by part (1) of Lemma 3.2.2,

$$\det\big(B[\alpha|\beta]\big) = -\det\big(A[\alpha|\beta]\big) \in DI_r(A).$$

(c) Suppose only one of the i_p and i_q belongs to $\{i_1, i_2, \ldots, i_r\}$, say i_p, i.e. $\alpha = (i_1, \ldots, i_p, \ldots, i_r)$. Setting $\alpha' = (i_1, \ldots, i_q, \ldots, i_r)$, different from α only by its p-th coordinate which is now i_q, then $B[\alpha|\beta] = A[\alpha'|\beta]$ and so,

$$\det\big(B[\alpha|\beta]\big) = \det\big(A[\alpha'|\beta]\big) \in DI_r(A).$$

Case 2: Suppose E multiplies row i_p of A by a unit $u \in R$ (units in $R = \mathbb{F}[x_1, \ldots, x_k]$ are nonzero elements in $\mathbb{F}$).

(a) If i_p is not in the coordinate of α, i.e. $i_p \notin \{i_1, i_2, \ldots, i_r\}$, then $\text{row}(i_p, A) = \text{row}(i_p, B)$, and so

$$\det\big(B[\alpha|\beta]\big) = \det\big(A[\alpha|\beta]\big) \in DI_r(A).$$

(b) If i_p is in the coordinate of α, i.e. $i_p \in \{i_1, i_2, \ldots, i_r\}$, then by part (2) of Lemma 3.2.2,

$$\det\big(B[\alpha|\beta]\big) = u \det\big(A[\alpha|\beta]\big) \in DI_r(A).$$

Case 3: Suppose E adds a multiple of row i_p of A to row i_q ($p \neq q$) of A.

(a) If both i_p and i_q do not belong to $\{i_1, i_2, \ldots, i_r\}$, then $\text{row}(i_p, A) = \text{row}(i_p, B)$ and $\text{row}(i_q, A) = \text{row}(i_q, B)$, and so

$$\det\big(B[\alpha|\beta]\big) = \det\big(A[\alpha|\beta]\big) \in DI_r(A).$$

(b) If both i_p and i_q belong to $\{i_1, i_2, \ldots, i_r\}$, then by part (3) of Lemma 3.2.2,

$$\det\big(B[\alpha|\beta]\big) = \det\big(A[\alpha|\beta]\big) \in DI_r(A).$$

(c) Suppose only one of the row indices i_p and i_q of A belongs to $\{i_1, i_2, \ldots, i_r\}$. First, if i_p only belongs to $\{i_1, i_2, \ldots, i_r\}$, then after the action of E on A, the submatrix $A[\alpha|\beta]$ remains unchanged, and so

$$\det\big(B[\alpha|\beta]\big) = \det\big(A[\alpha|\beta]\big) \in DI_r(A).$$

But if only i_q belongs to $\{i_1, i_2, \ldots, i_r\}$, setting $A[\alpha|\beta] = (A_{i_1}, \ldots, A_{i_q}, \ldots, A_{i_r})$, then

$$B[\alpha|\beta] = (A_{i_1}, \ldots, r\,A_{i_p} + A_{i_q}, \ldots, A_{i_r}),$$

$r \in R$. It therefore follows from properties (a) and (b) of Definition 3.2.1 that

$$\begin{aligned}\det\big(B[\alpha|\beta]\big) &= \det(A_{i_1}, \ldots, r\,A_{i_p} + A_{i_q}, \ldots, A_{i_r}) \\ &= r\,\det(A_{i_1}, \ldots, A_{i_p}, \ldots, A_{i_r}) + \det(A_{i_1}, \ldots, A_{i_q}, \ldots, A_{i_r}) \\ &= r\,\det\big(A[\alpha'|\beta]\big) + \det\big(A[\alpha|\beta]\big) \in DI_r(A),\end{aligned}$$

where $A[\alpha'|\beta]$ is another $r \times r$ submatrix of A which differs from $A[\alpha|\beta]$ by a row.

From the three cases considered above, we conclude that $DI_r(EA) \subseteq DI_r(A)$. On the other hand, let $B = EA$, then by the same concept above, we obtain $DI_r(E^{-1}B) \subseteq DI_r(B)$, reason being that the inverse of an elementary (row operation) matrix is also an elementary (row operation) matrix by Lemma 3.2.13. Therefore, substituting EA for B in the last (ideal) inclusion, we finally obtain $DI_r\big(E^{-1}(EA)\big) \subseteq DI_r(EA)$, i.e. $DI_r(A) \subseteq DI_r(EA)$. Hence, the result. □

The result above still remains true if only column operations are allowed. In other words, determinantal ideals are invariant under the right action of any elementary column operation matrix on an arbitrary matrix over R.

Remark 3.2.15. Let A be an $m \times n$ matrix over R. Also, let P be an arbitrary $m \times m$ elementary row operation matrix over R, and Q be an arbitrary $n \times n$ elementary column operation matrix over R. Let r be any positive integer such that $1 \leq r \leq \min\{m, n\}$. From Lemma 3.2.14 and the comment that follows it, we obtain

$$DI_r(PA) = DI_r(A), \quad \text{and} \quad DI_r(AQ) = DI_r(A).$$

Suppose that P' is another arbitrary $m \times m$ elementary row operation matrix over R. Then $DI_r\big(P'(PA)\big) = DI_r(PA)$, which implies $DI_r\big((P'P)A\big) = DI_r(A)$. Thus, if U is a product of some $m \times m$ elementary row operation matrices over R, we obtain $DI_r(UA) = DI_r(A)$. Similarly, if V is a product of some $n \times n$ elementary column operation matrices over R, we obtain $DI_r(AV) = DI_r(A)$. Therefore, for any matrix U that is a product of some elementary row operation matrices over R, and matrix V that is a product of some elementary column operation matrices over R, we obtain

$$DI_r(UAV) = DI_r\big((UA)V\big) = DI_r(UA) = DI_r(A),$$

i.e. $DI_r(UAV) = DI_r(A)$.

In the next result, we will show that the determinantal rank of any two equivalent matrices ($m \times n$ matrices A and B over R are said to be **equivalent** if $B = UAV$ for some invertible $n \times n$ matrix V over R and some invertible $m \times m$ matrix U over R) is invariant.

Corollary 3.2.16. *Let A be an arbitrary $m \times n$ matrix over R, U be any $m \times m$ matrix that is a product of some elementary row operation matrices over R, and V be any $n \times n$ matrix that is a product of some elementary column operation matrices over R. Then*

$$D\text{-}rank(UAV) = D\text{-}rank(A).$$

Proof. It has been shown that $DI_k(UA) = DI_k(A)$ for $k = 1, \ldots, \min\{m, n\}$ (Remark 3.2.15). Suppose D-rank$(UA) = r$, for some r, $1 \leq r \leq \min\{m, n\}$. Then by definition of determinantal rank, there exists a nonzero $r \times r$ minor of matrix UA, and in fact, r is the largest positive integer $\leq \min\{m, n\}$ such that there is a nonzero $r \times r$ minor of matrix UA. Consequently, there exist $\alpha \in \mathcal{C}(r, m)$ and $\beta \in \mathcal{C}(r, n)$ such that $\det\big(A[\alpha|\beta]\big) \in DI_r(UA)$ is nonzero. Since $DI_k(UA) = DI_k(A)$ for $k = 1, \ldots, \min\{m, n\}$, it implies the nonzero determinant $\det\big(A[\alpha|\beta]\big)$ also belongs to $DI_r(A)$. Therefore, we have found a nonzero $r \times r$ minor of matrix A, and so D-rank$(A) \geq r$, i.e. D-rank$(UA) \leq D$-rank(A). Similarly, we obtain D-rank$(AV) \leq D$-rank(A). Using the last two inequalities, we obtain D-rank$(UAV) = D$-rank$\big(U(AV)\big) \leq D$-rank(AV), i.e.

$$D\text{-rank}(UAV) \leq D\text{-rank}(A), \tag{3.1}$$

Since both matrices U and V are invertible over R, being the products of some elementary matrices, there exist matrices U^{-1} and V^{-1}, which are the inverses of U and V respectively, over R. Also, both U^{-1} and V^{-1} are products of some elementary matrices over R, and so we obtain D-rank$(A) = D$-rank$(U^{-1}UAVV^{-1}\big) \leq D$-rank$\big(U^{-1}(UAVV^{-1})\big) \leq D$-rank$(UAVV^{-1})$ $= D$-rank$\big((UAV)V^{-1}\big) \leq D$-rank$(UAV)$, i.e.

$$D\text{-rank}(A) \leq D\text{-rank}(UAV). \tag{3.2}$$

Now, combining inequalities (3.1) and (3.2), we finally obtain

$$D\text{-rank}(UAV) = D\text{-rank}(A),$$

as required. □

So far, the theory of determinantal ideals has only helped to study ranks of matrices over $\mathbb{F}[x_1, \ldots, x_k]$ as a function of the parameters (or variables) $x_1, \ldots, x_k$, but it does not help to determine ranks of these matrices when their parameters are only indeterminates, i.e. when values cannot be assigned to their parameters. Thus, for better understanding of ranks of matrices over the polynomial ring $\mathbb{F}[x_1, \ldots, x_k]$, $k \geq 2$, there is a need to review some theory of modules.

3.3 Brief theory of modules in relation to matrix rank

In this section, we present a brief summary of the theory of modules in relation to the question of the ranks of matrices over a polynomial ring in k indeterminates. We recall that for polynomials in one indeterminate with coefficients in a field, the polynomial ring is a principal ideal domain (PID), and so some of the main results of linear algebra over a field still hold, though their proofs require much more care. For example, if R is a PID, then (i) every submodule of a free R-module is also free, and (ii) every finitely generated torsion-free R-module is free. These conclusions do not follow if R is not a PID, as can be seen from the example $R = \mathbb{Z}[x]$, which is not a PID; the ideal $I = \langle 2, x \rangle \subseteq \mathbb{Z}[x]$, for example, is not principal. Since $R = \mathbb{Z}[x]$ is an integral domain, the ideal I (which is finitely generated by 2 and x) is torsion-free as an R-module, though it is not a free R-module. To see that I is not a free R-module, we first note that any generating set for I as an R-module must have at least two elements (this is the same as saying that I is not principal). But any two elements $f, g \in I$ are linearly dependent for the trivial reason that $gf - fg = 0$, which shows that any generating set for I is linearly dependent. More results along these lines and their proofs can be found in Sections 3.7 and 3.8 of [1]. The situation changes radically when we consider polynomials in two or more indeterminates over a field. The primary reference for this section is Adkins and Weintraub [1]; other sources will be cited when they are used. Henceforth, R will represent a commutative ring with identity 1, unless otherwise stated.

Definition 3.3.1. A **module** over R, written ***R*-module**, is an abelian group M together with a left action of R on M, that is, a function $R \times M \to M$, denoted $(r, m) \mapsto rm \in M$ ($r \in R$, $a \in M$), satisfying the following axioms: For arbitrary elements $r, r_1, r_2 \in R$ and

$m, m_1, m_2 \in M$,

(1) $r(m_1 + m_2) = rm_1 + rm_2$.

(2) $(r_1 + r_2)m = r_1m + r_2m$.

(3) $(r_1r_2)m = r_1(r_2m)$.

(4) $1m = m$.

Definition 3.3.2. Let M be an R-module. A **submodule** (written ***R*-submodule**, sometimes) of M is a subset $N \subseteq M$ which is also an R-module in its own right with respect to the operations already defined on R and M. In other words, N is an R-submodule of M if and only if N is an additive subgroup of M and it is closed under the action of R, i.e. $rm \in N$, for all $m \in N$ and $r \in R$.

Lemma 3.3.3. *If M is an R-module and N is a nonempty subset of M, then N is an R-submodule of M if and only if $rm - m' \in N$ for all $m, m' \in N$ and $r \in R$.*

Proof. Suppose a nonempty subset $N \subseteq M$ is an R-submodule of M. Then N is an R-module in its own right, and so for any elements $m, m' \in N$, $rm - m'$ belongs to N, for all $r \in R$. This is true since both rm and $-m'$ belong to N, N being an R-module. Conversely, suppose $rm - m'$ belongs to N for all $m, m' \in N$ and $r \in R$. Setting $r = 1$, then $m - m'$ belongs to N, showing that N is an additive subgroup of M. This further implies that 0 belongs to N, since $m - m = 0$. Lastly, taking m' to be 0, it implies that rm belongs to N, showing that N is closed under the action of R. □

Example 3.3.4. Let R be a commutative ring and let I be an ideal in R. If M is an R-module, then the set

$$IM = \left\{ \sum_{i=1}^{n} r_i m_i \ : \ n \in \mathbb{N},\ r_i \in I,\ m_i \in M \right\}$$

is a submodule of M. To verify this, by the lemma above, it suffices to show that $ra - b$ belongs to IM for all $a, b \in IM$ and $r \in R$. To this end, choose $a, b \in IM$ and $r \in R$ arbitrarily, then $a = \sum_{i=1}^{n} r_i m_i$ and $b = \sum_{j=1}^{n'} r'_j m'_j$ for some $n, n' \in \mathbb{N}$, $r_i, r'_j \in I$ and $m_i, m'_j \in M$. Thus,

$$ra - b = r\left(\sum_{i=1}^{n} r_i m_i \right) - \sum_{j=1}^{n'} r'_j m'_j = \sum_{i=1}^{n} (rr_i) m_i + \sum_{j=1}^{n'} (-r'_j) m'_j = \sum_{k=1}^{n''} r''_k m''_k,$$

which is an element in IM.

Let N be a submodule of an R-module M. Then N is an additive subgroup of M, and hence the set $M/N = \{m + N : m \in M\}$ is a quotient group. Define (left) action of R on M/N by $r(m + N) = rm + N$, for all $m \in M$ and $r \in R$. For m and m' in M, suppose $m + N = m' + N$. Then $m - m'$ belongs to N, implying $r(m - m')$ is in N since N is a submodule of M. Therefore, $rm - rm'$ belongs to N, and so $rm + N = rm' + N$, i.e. the action of R on M/N is well defined.

Definition 3.3.5. Let N be a submodule of an R-module M. The quotient group M/N constructed above is an R-module, and is called the **quotient module** of M by N.

Let $M_1, \ldots, M_k$ be finite collection of R-modules. Considering the Cartesian product $M = M_1 \times \cdots \times M_k$, we define addition on M component-wise by

$$(m_1, \ldots, m_k) + (m'_1, \ldots, m'_k) = (m_1 + m'_1, \ldots, m_k + m'_k),$$

and the (left) action of R on M by

$$r(m_1, \ldots, m_k) = (rm_1, \ldots, rm_k),$$

for any $(m_1, \ldots, m_k)$, $(m'_1, \ldots, m'_k) \in M$ and $r \in R$. The set $M = M_1 \times \cdots \times M_k$ is an abelian group with zero element $(0, \ldots, 0)$, since each M_i $(1 \leq i \leq k)$ is an abelian group with zero element 0. In addition, the set M satisfies axioms (1) to (4) of Definition 3.3.1, and hence, is an R-module.

Definition 3.3.6. The R-module constructed above is called the **direct product** (or **external direct sum**) of $M_1, \ldots, M_k$, denoted $M_1 \oplus \cdots \oplus M_k$.

Example 3.3.7.

(1) The (external) direct sum of n copies of R, denoted $R^n = R \oplus \cdots \oplus R$, is an R-module. It will be seen later that R^n is in fact the free R-module on a set of n free generators.

(2) In general, following the notation in Chapter 3 of [1], let I be a nonempty index set (finite or infinite) and $\{M_i\}_{i \in I}$ be a family of R-modules. Considering the Cartesian product $M = \prod_{i \in I} M_i$ of the M_i's, define addition and (left) action of R on M coordinate-wise by

$$(m_i)_{i \in I} + (m'_i)_{i \in I} = (m_i + m'_i)_{i \in I}, \qquad r(m_i)_{i \in I} = (rm_i)_{i \in I},$$

where $(m_i)_{i\in I}, (m_i')_{i\in I} \in M$ and $r \in R$. With this addition and R-action defined on M, M becomes an R-module, called the **direct product** of the R-modules M_i. Furthermore, considering the subset $\bigoplus_{i\in I} M_i$ of M which contains all element $(m_i)_{i\in I}$ in M with $m_i = 0$ except for finitely many indices $i \in I$, this subset $\bigoplus_{i\in I} M_i \subseteq M$ turns out to be a submodule of M, and therefore an R-module in its own right with respect to component-wise addition and R-action defined on M. The set $\bigoplus_{i\in I} M_i \subseteq \prod_{i\in I} M_i$ is the **direct sum** of the family $\{M_i\}_{i\in I}$ of R-modules. This coincides with the previous definition of direct product when the index set I is finite.

Definition 3.3.8. Let I be a nonempty index set (finite or infinite) and $\{M_i\}_{i\in I}$ be a family of R-submodules of R-module M. If every $m \in M$ can be written uniquely as a finite sum of elements of M_i, then we say M is the **internal direct sum** of the M_i's.

Definition 3.3.9. Let M and N be R-modules. A map $\phi : M \to N$ is an ***R*-module homomorphism** if

(i) $\phi(m + m') = \phi(m) + \phi(m')$, for all $m, m' \in M$, and

(ii) $\phi(rm) = r\phi(m)$, for all $m \in M$ and for all $r \in R$.

Remark 3.3.10. Let ϕ be an arbitrary R-module homomorphism from M to N. Let 0_M and 0_N be zero elements in M and N respectively. From the above definition, if $m' = -m$, then $m + m' = 0_M$, and thus, we obtain

$$\phi(0_M) = \phi(m + m') = \phi(m) + \phi(m') = \phi(m) + \phi(-m) = \phi(m) - \phi(m) = 0_N,$$

i.e. $\phi(0_M) = 0_N$.

Lemma 3.3.11. *Let M and N be R-modules. A map $\phi : M \to N$ is an R-module homomorphism if and only if $\phi(rm + m') = r\phi(m) + \phi(m')$ for all $r \in R$ and for all $m, m' \in M$.*

Proof. Suppose $\phi : M \to N$ is an R-module homomorphism, and let m, m' be any elements in M and r be any element in R. M being an R-module implies $rm + m'$ belongs to M. Consequently, $\phi(rm + m') = \phi(rm) + \phi(m') = r\phi(m) + \phi(m')$, since $\phi : M \to N$ is an R-module homomorphism. Conversely, suppose $\phi(rm + m') = r\phi(m) + \phi(m')$ for all $r \in R$

and for all $m, m' \in M$. Setting $r = 1$, then we obtain property (i) of Definition 3.3.9. Setting $m' = 0$, then by Remark 3.3.10, we obtain property (ii) of Definition 3.3.9. Hence, $\phi : M \to N$ is an R-module homomorphism. □

Definition 3.3.12. Let M and N be R-modules, and $\phi : M \to N$ be an R-module homomorphism. The **kernel** of ϕ, denoted $\ker(\phi)$ is the set

$$\ker(\phi) = \{m \in M : \phi(m) = 0_N\}.$$

The **image** of ϕ, denoted $\mathrm{Im}(\phi)$ is the set

$$\mathrm{Im}(\phi) = \{n \in N : n = \phi(m) \text{ for some } m \in M\}.$$

Lemma 3.3.13. *Let M and N be R-modules, and $\phi : M \to N$ be an R-module homomorphism. The subsets $\ker(\phi) \subseteq M$ and $Im(\phi) \subseteq N$ are submodules of M and N respectively.*

Proof. Let a and b be any elements in $\ker(\phi)$ and r be an arbitrary element in R. Then it will be shown that $ra - b$ belongs to $\ker(\phi)$ by showing that $\phi(ra - b) = 0_N$. Since ϕ is an R-module homomorphism, and a and b belong to $\ker(\phi)$, it follows that $\phi(ra - b) = r\phi(a) - \phi(b) = r\,0_N - 0_N = 0_N$, as expected. Similarly, for arbitrary elements $a', b' \in \mathrm{Im}(\phi)$ and $r \in R$, we will show that $ra' - b'$ belongs to $\mathrm{Im}(\phi)$. To this end, since a' and b' belong to $\mathrm{Im}(\phi)$, it follows that $\phi(a) = a'$ and $\phi(b) = b'$ for some $a, b \in M$. Therefore, since ϕ is an R-module homomorphism, we obtain $ra' - b' = r\phi(a) - \phi(b) = \phi(ra - b)$, i.e. $ra' - b'$ belongs to $\mathrm{Im}(\phi)$, since $ra - b$ is an element in M. □

Definition 3.3.14. Let M be an R-module. An R-submodule M_1 of M is a **direct summand** of M if there exists an R-submodule M_2 of M such that M is the internal direct sum of M_1 and M_2. In this case, we say M_1 and M_2 are **complementary submodules of M**.

Example 3.3.15. The equality and the internal direct sum in the definition above is actually important, and cannot just be replaced by an isomorphism and external direct sum respectively. For example, let $M = \mathbb{Z} \times \mathbb{Z}$ be a $\mathbb{Z}$-module. Consider $\mathbb{Z}$-submodules $M_1 = \mathbb{Z} \times \{0\}$ and $M_2 = \{0\} \times 2\mathbb{Z}$ of M. Since $M_1 \cong \mathbb{Z}$ and $M_2 \cong \mathbb{Z}$ as $\mathbb{Z}$-modules, it follows that M is isomorphic to the external direct sum $M_1 \oplus M_2$. However, M is not the internal direct sum of M_1 and M_2, since for example $(3, 5)$ belongs to M, but it cannot even be written as sum of elements in M_1 and M_2, let alone uniquely. In other words, M_1 is not a complement of M_2 as $\mathbb{Z}$-submodules of M.

Definition 3.3.16. Let M be an R-module. A subset S of M is called a **basis** of M if,

(1) S **spans** (or **generates**) M as an R-module, i.e. every element $m \in M$ can be written as $m = \sum_{i=1}^{k} r_i s_i$ for some $s_1, \ldots, s_k \in S$ and $r_1, \ldots, r_k \in R$, and

(2) S is ***R*-linearly independent**, i.e. the equation $\sum_{i=1}^{k} r_i s_i = 0$, for every distinct elements $s_1, \ldots, s_k \in S$ and elements $r_1, \ldots, r_k \in R$, has only trivial solution $r_1 = \cdots = r_k = 0$.

Remark 3.3.17. In view of the definition above, any subset of an R-linearly independent set is itself R-linearly independent.

Proposition 3.3.18. *Let M be an R-module. A set $S \subseteq M$ is a basis of M if and only if every $m \in M$ can be written uniquely as $m = \sum_{i=1}^{k} r_i s_i$ for $s_1, \ldots, s_k \in S$ and $r_1, \ldots, r_k \in R$.*

Proof. Let I be a fixed index set and $S = \{s_i : i \in I\}$ be a basis of M. Then by property (1) of Definition 3.3.16, any element $m \in M$ can be written as $m = \sum_{i \in I} r_i s_i$ where finitely many r_i's are nonzero. Now, suppose same element $m \in M$ can be written as $m = \sum_{i \in I} r_i' s_i$ where finitely many r_i''s are nonzero. Thus,

$$0 = \sum_{i \in I} r_i s_i - \sum_{i \in I} r_i' s_i = \sum_{i \in I} \left(r_i - r_i'\right) s_i.$$

Therefore, by property (2) of Definition 3.3.16, we obtain the trivial solution $r_i - r_i' = 0$, i.e. $r_i = r_i'$ for all $i \in I$. Hence, the uniqueness. Conversely, suppose for every $m \in M$, m can be written uniquely as $m = \sum_{i=1}^{k} r_i s_i$, for (distinct) $s_1, \ldots, s_k \in S$ and $r_1, \ldots, r_k \in R$. Then property (1) of Definition 3.3.16 follows immediately from this hypothesis. The zero element in M can be written as $0 = \sum_{i=1}^{k} 0 s_i$, for any $s_1, \ldots, s_k \in S$. If $m = 0$, then $\sum_{i=1}^{k} r_i s_i = m = 0 = \sum_{i=1}^{k} 0 s_i$ implying (by uniqueness) that $r_1 = \cdots = r_k = 0$, i.e. S is R-linearly independent since distinct elements $s_1, \ldots, s_k$ are arbitrarily chosen. Hence, the result. □

Remark 3.3.19. A set that is not R-linearly independent is said to be ***R*-linearly dependent**. In other words, a subset S of an R-module M is said to be R-linearly dependent if there exist distinct elements $s_1, \ldots, s_k \in S$ and elements $r_1, \ldots, r_k \in R$, not all 0, such that the equation $\sum_{i=1}^{k} r_i s_i = 0$ holds. In view of this, any set S that contains at least one R-linearly dependent set is itself R-linearly dependent.

Definition 3.3.20. Let M be an R-module, and S be a finite subset of M. If S generates M, then M is said to be **finitely generated.**

Example 3.3.21.

(1) The direct sum of n copies of R, R^n is a finitely generated R-module; one of its bases is $S = \{e_1, \ldots, e_k\}$, where $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ with 1 in its i-th coordinate.

(2) In particular, from Example 3.3.7(2), let $M_i = R$ for all $i \in I$, I being any fixed index set. Then $N = \bigoplus_{i \in I} M_i$, which is the direct sum of copies of R, is an R-module. We recall that an element in N is of the form $(m_i)_{i \in I} \in M$ (where $M = \prod_{i \in I} R$ is the Cartesian product of copies of R) with $m_i = 0$ except for finitely many indices $i \in I$. Let $S = \{(\delta_{ij})_{j \in I}\}_{i \in I}$, where δ_{ij} is the Kronecker delta function. For example, if $I = \mathbb{N}$, then

$$S = S_{\mathbb{N}} = \{(\delta_{ij})_{j \in I}\}_{i \in I} = \{(1, 0, 0, \ldots), (0, 1, 0, \ldots), (0, 0, 1, \ldots), \ldots\},$$

where each element in $S_{\mathbb{N}}$ has single nonzero entry with value 1. Back to the set $S = \{(\delta_{ij})_{j \in I}\}_{i \in I}$, every element in N can be written uniquely as a finite R-linear combination of elements in S. Thus, by Proposition 3.3.18, S is a basis of N. In fact, it will be seen later that no finite set could be a basis for N. In other words, N is not finitely generated.

Definition 3.3.22. A **free *R*-module** is a pair (M, ι), where ι is a mapping from a set S to an R-module M and $\iota(S)$ is a spanning set for M, satisfying: for any R-module N and any map $f : S \to N$, there exists a unique R-module homomorphism $\tilde{f} : M \to N$ such that $\tilde{f} \circ \iota = f$.

Theorem 3.3.23. *[13, p. 181] Let M be an R-module. Then the following statements are equivalent.*

(1) M is isomorphic to direct sum of copies of R.

(2) M has a basis.

(3) M is a free R-module.

Proof. The proof of this equivalent statements follows the same argument given in the sketch of the proof of Theorem 2.1 (chapter 5) in [13].

(1) $\Rightarrow$ (2) Let N be a direct sum copies of R. Then from Example 3.3.21(2), the set $S_N = \{(\delta_{ij})_{j\in I}\}_{i\in I}$ is a basis for R-module N. Suppose M is isomorphic to N, and let $\phi : N \to M$ be a bijective R-module homomorphism. We claim that the set $S_M = \big\{\phi\big((\delta_{ij})_{j\in I}\big)\big\}_{i\in I}$ is a basis for M. This is verified as follows. Let $m \in M$ be arbitrarily chosen. Since ϕ is bijective, its inverse ϕ^{-1} exists, and so $\phi^{-1}(m)$ belongs to N. Since the set S_N is a basis of N, by Proposition 3.3.18, $\phi^{-1}(m)$ can be written uniquely as finite R-linear combination of elements in S_N. In other words, for some finite subset $I' \subseteq I$,

$$\phi^{-1}(m) = \sum_{i\in I'} r_i\,(\delta_{ij})_{j\in I}.$$

Therefore, since ϕ is an R-module homomorphism, we obtain

$$m = \phi\big(\phi^{-1}(m)\big) = \phi\left(\sum_{i\in I'} r_i\,(\delta_{ij})_{j\in I}\right) = \sum_{i\in I'} r_i\,\phi\big((\delta_{ij})_{j\in I}\big),$$

i.e. the element $m \in M$ is written uniquely as finite R-linear combination of elements in S_M, as expected.

(2) $\Rightarrow$ (3) Suppose M has a basis, and let $S \subseteq M$ be this basis. Furthermore, let $\iota : S \hookrightarrow M$ be an inclusion map. If $m \in M$ is arbitrarily chosen, then m can be written uniquely as finite R-linear combination of elements in S. Consequently, for any R-module N and any map $f : S \to N$, let $\tilde{f} : M \to N$ be a mapping defined by

$$\tilde{f}(m) = \sum_{i=1}^{k} r_i f(s_i),$$

where $m = \sum_{i=1}^{k} r_i s_i$ for $r_1, \ldots, r_k \in R$ and $s_1, \ldots, s_k \in S$. We thus claim here that $\tilde{f}$ is the unique R-module homomorphism with $\tilde{f} \circ \iota = f$. This claim is verified as follows: Let $m, m' \in M$ and $r \in R$ be arbitrarily chosen. Then both m and m' can be written uniquely as $m = \sum_{i=1}^{p} r_i s_i$ (for $r_1, \ldots, r_p \in R$ and $s_1, \ldots, s_p \in S$), and $m' = \sum_{i=1}^{q} r'_i s'_i$ (for $r'_1, \ldots, r'_q \in R$ and $s'_1, \ldots, s'_q \in S$). Therefore,

$$\begin{aligned}
\tilde{f}(rm + m') &= \tilde{f}\left(r\left(\sum_{i=1}^{p} r_i s_i\right) + \left(\sum_{i=1}^{q} r'_i s'_i\right)\right) = \tilde{f}\left(\sum_{i=1}^{p} (rr_i) s_i + \sum_{i=1}^{q} r'_i s'_i\right) \\
&= \sum_{i=1}^{p} (rr_i) f(s_i) + \sum_{i=1}^{q} r'_i f(s'_i) = r\left(\sum_{i=1}^{p} r_i f(s_i)\right) + \left(\sum_{i=1}^{q} r'_i f(s'_i)\right) \\
&= r\tilde{f}(m) + \tilde{f}(m').
\end{aligned}$$

In addition, every $s \in S$ can be written as $s = 1s$, and also for every $s \in S$, $\iota(s) = s$ since ι is an inclusion map. Consequently, for every $s \in S$, we obtain

$$(\tilde{f} \circ \iota)(s) = \tilde{f}\big(\iota(s)\big) = \tilde{f}(s) = \tilde{f}(1s) = 1f(s) = f(s),$$

i.e. $\tilde{f} \circ \iota = f$. Lastly, it will be shown that $\tilde{f}$ is unique. To this end, let $\tilde{g} : M \to N$ be another R-module homomorphism satisfying $\tilde{g} \circ \iota = f$. Thus, for every $s \in S$, $(\tilde{f} \circ \iota)(s) = f(s) = (\tilde{g} \circ \iota)(s)$, i.e. $\tilde{f}\big(\iota(s)\big) = \tilde{g}\big(\iota(s)\big)$, i.e. $\tilde{f}(s) = \tilde{g}(s)$. Since $\tilde{g}$ is an R-module homomorphism, we obtain the following: for any $m = \sum_{i=1}^{k} r_i s_i \in M$,

$$\tilde{g}(m) = \tilde{g}\left(\sum_{i=1}^{k} r_i s_i\right) = \sum_{i=1}^{k} r_i \tilde{g}(s_i) = \sum_{i=1}^{k} r_i \tilde{f}(s_i) = \sum_{i=1}^{k} r_i \tilde{f}\big(\iota(s_i)\big)$$

$$= \sum_{i=1}^{k} r_i \big(\tilde{f} \circ \iota\big)(s_i) = \sum_{i=1}^{k} r_i f(s_i) = \tilde{f}(m).$$

(3) $\Rightarrow$ (1) Suppose (M, ι) is a free R-module, where ι is a mapping from an arbitrary set $S = \{s_i : i \in I\}$ to an R-module M and $\iota(S)$ generates M. Let $N = \oplus_{i \in I} R$ be copies of R (the number of R being the number of elements in S). Define an injection map

$$f : S \to N, \qquad s_i \mapsto (\delta_{ij})_{j \in I},$$

from set S into R-module N, where $T = \{(\delta_{ij})_{j \in I} : i \in I\}$ is a basis for N. Suppose $\tilde{f} : M \to N$ is an R-module homomorphism such that $\tilde{f} \circ \iota = f$. Then we will show that $\tilde{f}$ is in fact an isomorphism. But before then, it is important to note that if $\tilde{f} : M \to N$ is an R-module homomorphism with $\tilde{f} \circ \iota = f$, then $\iota(S) \subseteq M$ is an R-linearly independent set. In fact, for any distinct elements $\iota(s_1), \ldots, \iota(s_k) \in \iota(S)$ and elements $r_1, \ldots, r_k \in R$, if $\sum_{i=1}^{k} r_i\, \iota(s_i) = 0_M$, then by the definition of R-module homomorphism, we obtain the following:

$$\tilde{f}\left(\sum_{i=1}^{k} r_i\, \iota(s_i)\right) = \tilde{f}(0_M) = 0_N \implies \sum_{i=1}^{k} r_i\, \tilde{f}\big(\iota(s_i)\big) = 0_N \implies \sum_{i=1}^{k} r_i\, f(s_i) = 0_N$$

$$\implies \sum_{i=1}^{k} r_i\, (\delta_{ij})_{j \in I} = 0_N \implies r_1 = \cdots = r_k = 0,$$

since $T \subseteq N$ is an R-linearly independent set. Hence, by Proposition 3.3.18, the set $\iota(S) \subseteq M$ is a basis for M, and its cardinality equals to cardinality of the basis T of N. Consequently, every $m \in M$ can be written uniquely as finite R-linear combination of

elements in $\iota(S)$, i.e. $m = \sum_{i=1}^{k} r_i\, \iota(s_i)$, for $\iota(s_1), \ldots, \iota(s_k) \in \iota(S)$ and $r_1, \ldots, r_k \in R$, implying

$$\tilde{f}(m) = \tilde{f}\left(\sum_{i=1}^{k} r_i\, \iota(s_i)\right) = \sum_{i=1}^{k} r_i\, \tilde{f}\big(\iota(s_i)\big) = \sum_{i=1}^{k} r_i\, f(s_i) = \sum_{i=1}^{k} r_i\, (\delta_{ij})_{j\in I}.$$

It will now be shown that $\tilde{f}$ is bijective. Every element $(a_i)_{i\in I}$ in N can be written uniquely as finite R-linear combination of elements in $T = \{(\delta_{ij})_{j\in I} : i \in I\} \subseteq N$, i.e. $(a_i)_{i\in I} = \sum_{i=1}^{k} r'_i\, (\delta_{ij})_{j\in I}$, for $(\delta_{1j})_{j\in I}, \ldots, (\delta_{kj})_{j\in I} \in T$ and $r'_1, \ldots, r'_k \in R$, and so for this unique $r'_1, \ldots, r'_k \in R$, the element $\sum_{i=1}^{k} r'_i\, \iota(s_i)$ belongs to M with

$$\tilde{f}\left(\sum_{i=1}^{k} r'_i\, \iota(s_i)\right) = \sum_{i=1}^{k} r'_i\, (\delta_{ij})_{j\in I} = (a_i)_{i\in I},$$

i.e. $\tilde{f}$ is surjective. Furthermore, $\tilde{f}$ is injective since $\ker(\tilde{f}) = \{0_M\}$. In fact,

$$\begin{aligned}
\ker(\tilde{f}) &= \{m \in M : \tilde{f}(m) = (0)_{i\in I} = 0_N\} \\
&= \left\{m = \sum_{i=1}^{k} r_i\, \iota(s_i) : \tilde{f}\left(\sum_{i=1}^{k} r_i\, \iota(s_i)\right) = 0_N\right\} \\
&= \left\{m = \sum_{i=1}^{k} r_i\, \iota(s_i) : \sum_{i=1}^{k} r_i (\delta_{ij})_{j\in I} = 0_N\right\} \\
&= \left\{m = \sum_{i=1}^{k} r_i\, \iota(s_i) : r_1 = \cdots = r_k = 0\right\} = \{0_M\}.
\end{aligned}$$

This completes the proof. □

Definition 3.3.24. [13, p. 185] A ring R has **invariant basis number (IBN)** if for all positive integers k and l, R^k isomorphic to R^l (as left R-modules) implies that $k = l$.

Remark 3.3.25. In respect to the above definition, if R is a ring that satisfies the IBN property, and M is a free R-module with basis B, then, from Theorem 3.3.23, M is isomorphic to direct sum of copies of R, precisely $|B|$ copies of R, denoted $R^{|B|}$, where $|B|$ is the cardinality of B. Similarly, if M has another basis, say B', then M is isomorphic to $R^{|B'|}$. Together, we obtain $R^{|B|} \cong M \cong R^{|B'|}$, implying $|B| = |B'|$, since R satisfies the IBN property. In other words, *if a ring R satisfies the IBN property, then any two bases of any free R-module M must have the same cardinality.* On the other hand, let M be a free R-module having the property that if B and B' are any two bases of M, then B and B' have the same cardinality. For any positive integers k and l, suppose $\phi : R^k \to R^l$ is an isomorphism

of (free) R-modules. Let B and B' be standard bases for R^k and R^l respectively. The set $\phi(B) = \{\phi(b) : b \in B\}$ is also a basis for R^l since ϕ is an isomorphism. Hence, by our hypothesis, both B' and $\phi(B)$ have the same cardinality, i.e. $l = |B'| = |\phi(B)| = k$, i.e. $l = k$. In other words, *if R satisfies the condition that for every free R-module M, any two bases of M have the same cardinality, then R satisfies the IBN property.*

Considering the definition of IBN, a good question to ask is whether the polynomial ring $\mathbb{F}[x_1, \ldots, x_n]$ satisfies the IBN property? It turns out that the polynomial ring $\mathbb{F}[x_1, \ldots, x_n]$ actually satisfies the IBN property, reason being that it is a commutative ring with $1 \neq 0$. That every nonzero commutative ring satisfies the IBN property will be proven in a moment. But before considering the proof, it is important to note that every field satisfies the IBN property; reason being that any $\mathbb{F}$-module is a vector space over the field $\mathbb{F}$, and so any two bases for this vector space over the field $\mathbb{F}$ will have same cardinality. This fact (that every field satisfies the IBN property) and the Krull's theorem (stated below without proof) help in proving that every nonzero commutative ring does satisfy the IBN property.

Theorem 3.3.26. (Krull's theorem) *Every nonzero ring (with identity) has at least one maximal ideal.*

Remark 3.3.27. Krull's theorem was originally proven by Krull in 1929 [17]. Krull's proof was later simplified by Zorn in the paper which introduced what is now known as Zorn's Lemma [21]; Application I in this paper is a much shorter proof of Krull's theorem than was given by Krull in his original paper. The proof of Krull's theorem uses Zorn's lemma. In fact, the two statements are equivalent, as first shown by Hodges [11]. Banaschewski [2] later gave a new proof that Zorn's lemma follows from Krull's theorem. Further historical details are given by Campbell [5] and Erné [9].

The following result shows that every nonzero commutative ring satisfies the IBN property. The proof provided here is the same as the proof in [19] (Proposition 7.50), though the author left some facts as exercise. These facts are proven here, which makes the proof more complete.

Corollary 3.3.28. *If R is a nonzero commutative ring, then R satisfies the IBN property.*

Proof. Let R be a nonzero commutative ring. By Remark 3.3.25, in order to show that R satisfies the IBN property, it suffices to prove that for any free R-module M with bases

B and B', B and B' have the same cardinality. To this end, let M be a free R-module with basis B. By Krull's theorem, R has a maximal ideal, say I, implying R/I is a field. From Example 3.3.4, IM is a submodule of M. We thus claim that the quotient group M/IM is an R/I-module, and hence a vector space over R/I (R/I being a field) with a basis $F = \{b + IM \ : \ b \in B\}$. In fact, M/IM is an abelian group (since M is abelian), and if we define a (left) action of R/I on M/IM by $(r + I)(m + IM) = rm + IM$, for all $m \in M$ and $r \in R$, then, in addition, M/IM satisfies axioms (1) to (4) of Definition 3.3.1. Hence, M/IM is a vector space over the field R/I. It will now be shown that the set F is indeed a basis for M/IM, by showing that F is an R/I-linearly independent set, and in addition generates M/IM as a vector space over the field R/I. First, every element in M/IM is of the form $m + IM$, where m belongs to M. Since B is a basis for M as an R-modules, it implies $m = \sum_{i=1}^{k} r_i b_i$ for some $r_1, \ldots, r_k \in R$ and $b_1, \ldots, b_k \in B$. Thus,

$$m + IM = \left(\sum_{i=1}^{k} r_i b_i \right) + IM = \sum_{i=1}^{k} (r_i b_i + IM) = \sum_{i=1}^{k} \left[(r_i + I)\,(b_i + IM) \right],$$

i.e. the set $F = \{b + IM : b \in B\}$ generates M/IM as a vector space over the field R/I. Next, suppose for distinct elements $b_1 + IM, \ldots, b_k + IM \in F$ and elements $r_1 + I, \ldots, r_k + I \in R/I$, the equation $\sum_{i=1}^{k} [(r_i + I)(b_i + IM)] = IM = 0 + IM$ holds. Then

$$\left(\sum_{i=1}^{k} r_i b_i \right) + IM = 0 + IM \quad \Longrightarrow \quad \sum_{i=1}^{k} r_i b_i \in IM \quad \Longrightarrow \quad r_1, \ldots, r_k \in I,$$

i.e. the equation $\sum_{i=1}^{k} [(r_i + I)(b_i + IM)] = IM$ has only trivial solution $r_1 + I = \cdots = r_k + I = 0 + I = I$, i.e. the set F is an R/I-linearly independent set. Therefore, F is a basis for vector space M/IM over the field R/I. Similarly, if B' is another basis of free R-module M, then the set $F' = \{b' + IM \ : \ b' \in B'\}$ is a basis for the vector space M/IM over the field R/I. R/I being a field implies it satisfies the IBN property, and consequently, the two bases F and F' of the vector space M/IM over the field R/I must have same cardinality. But the cardinality of F is just the same as cardinality of B, and also the cardinality of F' is just the same as cardinality of B'. Therefore, $|B| = |B'|$, as expected. □

Example 3.3.29. In this example, a ring that does not satisfy the IBN property is given. Let $\mathbb{N}$ be the set of natural numbers, and R be an arbitrary ring. Also, let $\mathbb{CFM}_{\mathbb{N}}(R)$ be the set of all (infinite) matrices over R, whose entries are indexed by $\mathbb{N} \times \mathbb{N}$, and whose columns

contain finitely many nonzero entries [6]. Define addition and multiplication on $\mathbb{CFM}_{\mathbb{N}}(R)$ by:

$$(A+B)_{ij} = a_{ij} + b_{ij}, \qquad (AB)_{ij} = \sum_{k\in\mathbb{N}} a_{ik}\, b_{kj},$$

for all matrices $A = (a_{ij})$ and $B = (b_{ij})$ in $\mathbb{CFM}_{\mathbb{N}}(R)$. With these definitions, $\mathbb{CFM}_{\mathbb{N}}(R)$ becomes a (noncommutative) ring. Let $f\colon \mathbb{CFM}_{\mathbb{N}}(R) \to \mathbb{CFM}_{\mathbb{N}}(R)$ be a map that takes any infinite matrix A as an input, and output an infinite matrix B whose columns are the odd-numbered columns of the infinite matrix A. Similarly, let $g\colon \mathbb{CFM}_{\mathbb{N}}(R) \to \mathbb{CFM}_{\mathbb{N}}(R)$ be a map that takes any infinite matrix A as an input, and output an infinite matrix B whose columns are the even-numbered columns of the infinite matrix A. Both maps f and g are left $\mathbb{CFM}_{\mathbb{N}}(R)$-module isomorphisms. Therefore, the map

$$\phi\colon \mathbb{CFM}_{\mathbb{N}}(R) \to \mathbb{CFM}_{\mathbb{N}}(R)^2$$

defined by

$$\phi(A) = \big(f(A), g(A)\big),$$

is a left $\mathbb{CFM}_{\mathbb{N}}(R)$-module isomorphism. In other words,

$$\mathbb{CFM}_{\mathbb{N}}(R) \cong \mathbb{CFM}_{\mathbb{N}}(R)^2$$

i.e. $\mathbb{CFM}_{\mathbb{N}}(R)^1$ is isomorphic to $\mathbb{CFM}_{\mathbb{N}}(R)^2$ as left $\mathbb{CFM}_{\mathbb{N}}(R)$-modules, but obviously $1 \neq 2$ as (positive) integers. Hence, the ring $\mathbb{CFM}_{\mathbb{N}}(R)$ does not satisfy the invariant basis number (IBN) property.

Definition 3.3.30. Let A be an $m \times n$ matrix over the polynomial ring R. The submodule of R^n generated by the m rows of A is called the **row module of $\boldsymbol{A}$**, denoted **rowmod($\boldsymbol{A}$)**. It is the analogue of the row space of a matrix over a field.

Let $R = \mathbb{F}[x_1, \ldots, x_k]$, where $\mathbb{F}$ is a field, be the ring of polynomials in k indeterminates. As a result of Corollary 3.3.28, every free R-module has a well-defined **rank (or dimension)**, where rank is defined to be the cardinality of any (module) basis of the free R-module. This shows that the R-module N considered in Example 3.3.21 (2) is indeed not finitely generated. But what can be said about rank of an arbitrary finitely generated submodule of a free module? As said earlier, of much interest to us is computing rank (if possible) of an arbitrary $m \times n$ matrix over the polynomial ring R. If A is an $m \times n$ matrix over the polynomial ring R, then rowmod(A) is finitely generated. So we wish to know the rank (if

possible) of rowmod(A) as a finitely generated submodule of the free R-module R^n. It is important to note that not every submodule of R^n is a free R-module. An example is given below to support this claim.

Example 3.3.31. Let $R = \mathbb{F}[x_1, \ldots, x_k]$, where $k \geq 2$ and $\mathbb{F}$ is a field, and let

$$A = \begin{bmatrix} x_1 \\ \vdots \\ x_k \end{bmatrix}$$

be a $k \times 1$ matrix over the polynomial ring R. Here, rowmod (A) is a finitely generated (since $m = k$) submodule of free R-module R^n, where $n = 1$. Since $n = 1$, submodules of $R^n = R$ are just ideals in R. In other words, rowmod (A) is just an ideal of R generated by finite set $\{x_1, \ldots, x_k\}$. First, the set $\{x_1, \ldots, x_k\}$ is not a basis for rowmod(A) since it is an R-linearly dependent set. In fact, the relation $(-x_i) \cdot x_j + x_j \cdot x_i = 0$, where $\cdot$ denotes the left action of R on rowmod (A), holds for any x_i and x_j, $1 \leq i, j \leq k$, and none of $-x_i$ and x_j is zero in R, showing that any subset $\{x_i, x_j\}_{i \neq j} \subseteq \{x_1, \ldots, x_k\}$ is truly not R-linearly independent. Consequently, the set $\{x_1, \ldots, x_k\}$ itself is not R-linearly independent, by Remark 3.3.19. Next, no two elements of rowmod (A) are R-linearly independent. This is true since for any elements f and g in rowmod (A) (in fact, for any elements f and g in R), the relation $(-g)f + fg = 0$ always holds, implying by Remark 3.3.19 that every set containing more than 1 element of rowmod (A) is R-linearly dependent. Lastly, it will be shown that rowmod (A) is not principal. Suppose by contradiction, rowmod (A) is principal. Then there exists an element $f \in$ rowmod (A) such that rowmod $(A) = Rf = \{rf : r \in R\}$. This implies that all $x_1, \ldots, x_k$ belong to Rf. For a fixed i, $1 \leq i \leq k$, that x_i is in Rf implies that $x_i = rf$ for some $r \in R$, which further implies that either $f = cx_i$ for some nonzero $c \in \mathbb{F}$ or f is just a nonzero constant in $\mathbb{F}$. However, since elements in rowmod (A) are polynomials in $x_1, \ldots, x_k$ with zero constant term, it implies that $f = cx_i$ for some nonzero $c \in \mathbb{F}$. Consequently, any x_j, $1 \leq j \neq i \leq k$ (i.e. any x_j different from x_i) does not belong to Rf, since there exists no $r \in R$ such that $x_j = rf = crx_i$ for all $c \in \mathbb{F}$. This is a contradiction since x_j actually belongs to rowmod (A). This shows that no singleton subset (different from $\{0\}$) of rowmod (A) generates rowmod (A), though every singleton nonzero subset of rowmod (A) is R-linearly independent (since R is an integral domain). Therefore, rowmod (A) is not a free R-module.

Now, let $R = \mathbb{F}[x_1, \ldots, x_k]$, where $\mathbb{F}$ is a field. Then we claim that not every submodule of the free R-module R^n is a free R-module. Suppose $p \leq n$. Let S be the subset of R^n containing elements of the form $(r_1, \ldots, r_p, 0, \ldots, 0)$, where the first p components are any elements in R and the last $n-p$ elements are zero. The set S is a submodule of R^n, and it is a free R-module generated by $\{e_1, \ldots, e_p\}$, where $e_i \, (1 \leq i \leq p)$ is an element in R^n with 1 at the i-th position and 0 elsewhere. Furthermore, R^p is isomorphic to $S \subseteq R^n$ (as R-modules) by the map

$$(r_1, \ldots, r_p) \leftrightarrow (r_1, \ldots, r_p, 0, \ldots, 0).$$

In particular, setting p to be 1, then free R-module $R^p = R$ is isomorphic to some free R-module $S \subseteq R^n$. Due to this just mentioned isomorphism and Example 3.3.31, there exists a submodule, say T, of the free R-module S that is not a free R-module. Since the submodule T of the free R-module S is also a submodule of the free R-module R^n, we conclude that not every submodule of the free R-module R^n is a free R-module.

Example 3.3.32. Let $R = \mathbb{F}[x, y]$, where $\mathbb{F}$ is a field. Considering the same matrix in the last example above, it will be shown that the submodule $\text{rowmod}\,(A)$ of free R-module R is not a direct summand of R. In other words, $\text{rowmod}\,(A)$ has no complementary submodule. Suppose $\text{rowmod}\,(A)$ has a complementary submodule, say submodule $S \subseteq R$. Then, by definition, R is isomorphic to $\text{rowmod}\,(A) \oplus S$, as R-modules. Restricting to $\mathbb{F}$ the action of $R = \mathbb{F}[x, y]$ on these R-modules, then these R-modules can be regarded as vector spaces over the field $\mathbb{F}$, and consequently, R is now isomorphic to $\text{rowmod}\,(A) \oplus S$, as vector spaces over $\mathbb{F}$, implying $R/\text{rowmod}\,(A) \cong S$, as vector spaces over the field $\mathbb{F}$. Elements in the $\mathbb{F}$-vector space $R/\text{rowmod}\,(A)$ are of the form $f + \text{rowmod}\,(A)$, where f is any polynomial in R with nonzero constant term, thereby making the singleton set $\{1 + \text{rowmod}\,(A)\}$ a basis for $R/\text{rowmod}\,(A)$, i.e. $R/\text{rowmod}\,(A)$ is a 1-dimensional vector space over the field $\mathbb{F}$. As a result of this, S is a 1-dimensional vector space over the field $\mathbb{F}$, since $R/\text{rowmod}\,(A) \cong S$. One possibility of S is $\mathbb{F}$, and in general, S could be $\mathbb{F}f = \{cf \, : \, c \in \mathbb{F}\}$, where f is any polynomial in R with nonzero constant term. Therefore, substituting $\mathbb{F}$ for S in the R-module isomorphism $R \cong \text{rowmod}\,(A) \oplus S$, we obtain $R \cong \text{rowmod}\,(A) \oplus \mathbb{F}$, as R-modules. This is a contradiction, since $\mathbb{F}$ is not an R-module, as it is not closed under the action of R. In general, the $\mathbb{F}$-vector space $\mathbb{F}f$, where f is any polynomial in R, is not an R-module, reason

being that not every polynomial in R is a scalar multiple of f. Hence, rowmod (A) has no complementary submodule, and so it is not a direct summand of free R-module R.

Chapter 4

Analogue of Smith normal form for polynomial matrix

Let $\mathbb{F}$ be a field. For the ring of polynomials $\mathbb{F}[x]$ in one indeterminate x, the concept of **Smith Normal Form (SNF)** does make sense, since $\mathbb{F}[x]$ is a Euclidean domain, and hence, a PID. However, when there is more than one indeterminate, the concept of SNF becomes undefined. In a case whereby an arbitrary matrix over the polynomial ring $\mathbb{F}[x_1, \ldots, x_k]$, $k \geq 2$ contains sufficiently many nonzero scalars (elements in $\mathbb{F}$), an analogue of the SNF, called **Partial Smith Form (PSF)** [3], can be applied to such matrix. The resulting matrix gives some information on how the rank of the matrix depends on the values of the indeterminates. In this chapter, the theory of Smith normal form of matrices over the polynomial ring in one indeterminate over the field $\mathbb{F}$, will be discussed. This theory will later be extended to partial Smith normal form of matrices (with many nonzero scalars as entries) in two or more indeterminates over the field $\mathbb{F}$. The major references for this chapter are [3] and [18].

4.1 Smith normal form of a matrix over $\mathbb{F}[x]$

In this section, we give a brief summary of the theory of Smith normal form of matrices over the ring of polynomials in one indeterminate with coefficients in a field.

Definition 4.1.1. Let $S = (s_{ij})$ be an $m \times n$ matrix over $\mathbb{F}[x]$ satisfying:
(1) S is a diagonal matrix, i.e. $s_{ij} = 0$ for all $i \neq j$,
(2) there exists a non-negative integer $r \leq \min\{m, n\}$ such that s_{ii} is monic for $1 \leq i \leq r$, and $s_{ii} = 0$ for $r + 1 \leq i \leq \min\{m, n\}$,
(3) setting $f_i = s_{ii}$ for $1 \leq i \leq r$, then $f_i \mid f_{i+1}$ (f_{i+1} is divisible by f_i) for $1 \leq i \leq r - 1$.

Then the matrix

$$S = \begin{bmatrix} f_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & f_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & f_r & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix}$$

is said to be in **Smith normal form** (abbreviated SNF).

The following result helps in proving the existence of the Smith normal form of an arbitrary matrix over $\mathbb{F}[x]$.

Lemma 4.1.2. *Let $A = (a_{ij})$ be a 2×2 diagonal matrix over $\mathbb{F}[x]$ with at least one nonzero entry, and d be the greatest common divisor of the diagonal entries of A (i.e. $d = \gcd(a_{11}, a_{22})$). Then there exist 2×2 invertible matrices U and V over $\mathbb{F}[x]$ and an element $d' \in \mathbb{F}[x]$ such that*

$$UAV = \begin{bmatrix} d & 0 \\ 0 & d' \end{bmatrix},$$

and d divides d'.

Proof. Let

$$A = \begin{bmatrix} a_{11} & 0 \\ 0 & a_{22} \end{bmatrix}$$

be a 2×2 diagonal matrix over $\mathbb{F}[x]$ with at least one nonzero entry. If $a_{22} = 0$, then $d = a_{11}$, $U = V = I_2$, and $d' = 0$. But if $a_{11} = 0$, then $d = a_{22}$,

$$U = V = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

and $d' = 0$. Now, suppose a_{11} and a_{22} are both nonzero and monic. Since $\mathbb{F}[x]$ is a PID, we obtain $\langle a_{11}, a_{22}\rangle = \langle d\rangle$ by Theorem 2.1.6, where d is the greatest common divisor of the set $\{a_{11}, a_{22}\} \subseteq \mathbb{F}[x]$. In other words, d belongs to $\langle a_{11}, a_{22}\rangle$, and so there exists f and g in $\mathbb{F}[x]$ such that $d = fa_{11} + ga_{22}$. Consequently, we obtain the following:

$$A = \begin{bmatrix} a_{11} & 0 \\ 0 & a_{22} \end{bmatrix} \xrightarrow[AV_1=A_1]{V_1=\begin{bmatrix} 1 & f \\ 0 & 1 \end{bmatrix}} A_1 = \begin{bmatrix} a_{11} & fa_{11} \\ 0 & a_{22} \end{bmatrix} \xrightarrow[U_1A_1=A_2]{U_1=\begin{bmatrix} 1 & g \\ 0 & 1 \end{bmatrix}} A_2 = \begin{bmatrix} a_{11} & d = fa_{11} + ga_{22} \\ 0 & a_{22} \end{bmatrix}$$

$$A_2 = \begin{bmatrix} a_{11} & d \\ 0 & a_{22} \end{bmatrix} \xrightarrow[A_2V_2=A_3]{V_2=\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}} A_3 = \begin{bmatrix} d & a_{11} \\ a_{22} & 0 \end{bmatrix} \xrightarrow[A_3V_3=A_4]{V_3=\begin{bmatrix} 1 & -\frac{a_{11}}{d} \\ 0 & 1 \end{bmatrix}} A_4 = \begin{bmatrix} d & 0 \\ a_{22} & -\frac{a_{11}a_{22}}{d} \end{bmatrix}$$

$$A_4 = \begin{bmatrix} d & 0 \\ a_{22} & -\frac{a_{11}a_{22}}{d} \end{bmatrix} \xrightarrow[U_2A_4=A_5]{U_2=\begin{bmatrix} 1 & 0 \\ -\frac{a_{22}}{d} & 1 \end{bmatrix}} A_5 = \begin{bmatrix} d & 0 \\ 0 & -\frac{a_{11}a_{22}}{d} \end{bmatrix} \xrightarrow[U_3A_5=A_6]{U_3=\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}} A_6 = \begin{bmatrix} d & 0 \\ 0 & \frac{a_{11}a_{22}}{d} \end{bmatrix}$$

Setting

$$U := U_3U_2U_1 = \begin{bmatrix} 1 & g \\ \frac{a_{22}}{d} & \frac{a_{22}}{d}g-1 \end{bmatrix}, \qquad V := V_1V_2V_3 = \begin{bmatrix} f & 1-\frac{a_{11}}{d}f \\ 1 & -\frac{a_{11}}{d} \end{bmatrix},$$

then

$$UAV = \begin{bmatrix} d & 0 \\ 0 & d' \end{bmatrix},$$

where $d' = \frac{a_{11}a_{22}}{d}$, and indeed d divides d'. □

Combining Lemma 2.2.3, Remark 2.2.4, and Lemma 4.1.2, we give a proof for the existence of Smith normal form for an arbitrary matrix over $\mathbb{F}[x]$.

Theorem 4.1.3. *Let A be an $m \times n$ matrix over $\mathbb{F}[x]$. Then there exists an $m \times n$ matrix S over $\mathbb{F}[x]$ in Smith normal form such that $UAV = S$, for some $m \times m$ invertible matrix U over $\mathbb{F}[x]$ and some $n \times n$ invertible matrix V over $\mathbb{F}[x]$ (U is a product of elementary row operation matrices over $\mathbb{F}[x]$ and V is a product of elementary column operation matrices over $\mathbb{F}[x]$).*

Proof. The proof of this result is constructed based on Theorem 1.11 (existence of the SNF over the ring of integers, $\mathbb{Z}$) in [18]; there the author stated existence of the SNF over $\mathbb{F}[x]$ as Theorem 4.16, and then left the proof as an exercise, since it is similar to the proof of the existence of the SNF over the ring of integers, $\mathbb{Z}$. We proceed by induction on $k = \min\{m, n\}$. To this end, let $T(k)$ (where $k = \min\{m, n\}$) be the statement that for every $m \times n$ matrix A over $\mathbb{F}[x]$, there exists an $m \times n$ matrix S over $\mathbb{F}[x]$ in Smith normal form such that $UAV = S$, for some $m \times m$ invertible matrix U over $\mathbb{F}[x]$, and for some $n \times n$ invertible matrix V over $\mathbb{F}[x]$. For $k = 1$, i.e. $\min\{m, n\} = 1$, assume that $m = 1$, and let

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \end{bmatrix}$$

be a $1 \times n$ (nonzero) matrix over $\mathbb{F}[x]$. By Remark 2.2.4, if $d = \gcd(A)$, where d is monic, then there exist an $n \times n$ invertible matrix V over $\mathbb{F}[x]$ such that

$$AV = \begin{bmatrix} d & 0 & \cdots & 0 \end{bmatrix}.$$

Setting $U = I_1$ (the 1×1 identity matrix), then the matrix $UAV = S$ obviously satisfies Definition 4.1.1. Hence, $T(1)$ is true. Now, suppose that $T(k-1)$ is true for $k = \min\{m, n\} \geq 2$. Let

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

be an $m \times n$ matrix over $\mathbb{F}[x]$. By Lemma 2.2.3 and Remark 2.2.4, if

$$d = \gcd\left(\{a_{i1} \,:\, 1 \leq i \leq m\}, \{a_{1j} \,:\, 1 \leq j \leq n\}\right),$$

where d is monic, then there exist invertible matrices U_1 and V_1 over $\mathbb{F}[x]$ such that

$$U_1 A V_1 = A_1 = \begin{bmatrix} d & 0 & \cdots & 0 \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \cdots & * \end{bmatrix} = \begin{bmatrix} d & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{bmatrix}.$$

The submatrix B of matrix A_1 is an $(m-1) \times (n-1)$ matrix over $\mathbb{F}[x]$ and so by the induction hypothesis (since $\min\{m-1, n-1\} = \min\{m, n\} - 1 = k-1$), there exists an $(m-1) \times (n-1)$ matrix S' over $\mathbb{F}[x]$ in Smith normal form such that $WBW' = S'$, for some $(m-1) \times (m-1)$ invertible matrix W over $\mathbb{F}[x]$, and also for some $(n-1) \times (n-1)$ invertible matrix W' over $\mathbb{F}[x]$. That S' is in Smith normal form implies S' satisfies properties (1) - (3) of Definition 4.1.1. Setting

$$U_2 := \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & W & \\ 0 & & & \end{bmatrix}, \quad \text{and} \quad V_2 := \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & W' & \\ 0 & & & \end{bmatrix},$$

then the matrix

$$A_2 = U_2 A_1 V_2 = \begin{bmatrix} d & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & S' & \\ 0 & & & \end{bmatrix}$$

obviously satisfies properties (1) and (2) of Definition 4.1.1. It is only left to ensure that property (3) is satisfied. To this end, let

$$A_2 = \begin{bmatrix} d & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & s'_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 0 & s'_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & s'_{r-1} & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix},$$

where $s'_1, s'_2, \ldots, s'_{r-1}$ are nonzero (monic) diagonal entries of matrix S'. If $d \,|\, s'_1$, then the diagonal entries of A_2 will satisfy property (3) of Definition 4.1.1, and so the proof is complete. Otherwise, by Lemma 4.1.2, there exists 2×2 invertible matrices T and T' over $\mathbb{F}[x]$ and element $s''_1 \in \mathbb{F}[x]$ such that $f_1 = \gcd(d, s'_1)$ divides s''_1 (f_1 being monic), and

$$U_3 A_2 V_3 = A_3 = \left[\begin{array}{cc|ccccc} f_1 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & s''_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \hline 0 & 0 & s'_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & s'_{r-1} & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{array}\right], \text{ where } U_3 = \left[\begin{array}{c|c} T & 0 \\ \hline 0 & I_{m-2} \end{array}\right], \text{ and } V_3 = \left[\begin{array}{c|c} T' & 0 \\ \hline 0 & I_{n-2} \end{array}\right].$$

Rewriting matrix A_3 to be of the form

$$A_3 = \begin{bmatrix} f_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & B' & \\ 0 & & & \end{bmatrix},$$

the submatrix B' of matrix A_3, with nonzero diagonal entries $s''_1, s'_2, \ldots, s'_{r-1}$, is an $(m-1) \times (n-1)$ matrix over $\mathbb{F}[x]$ and so by the induction hypothesis, there exists an $(m-1) \times (n-1)$ matrix S'' over $\mathbb{F}[x]$ in Smith normal form such that $PB'Q = S''$, for some $(m-1) \times (m-1)$ invertible matrix P over $\mathbb{F}[x]$, and some $(n-1) \times (n-1)$ invertible matrix Q over $\mathbb{F}[x]$. Setting

$$U_4 := \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & P & \\ 0 & & & \end{bmatrix}, \quad \text{and} \quad V_4 := \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & Q & \\ 0 & & & \end{bmatrix},$$

then we claim that the matrix

$$U_4A_3V_4 = S = \begin{bmatrix} f_1 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & f_2 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 0 & f_3 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & f_r & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix},$$

where $f_2, f_3, \ldots, f_r$ are nonzero (monic) diagonal entries of matrix S'', is in Smith normal form. The matrix S obviously satisfies properties (1) and (2) of Definition 4.1.1. It is now left to verify that matrix S satisfies property (3). Since the submatrix S' of matrix A_2 is in Smith normal form, it implies by property (3) of Definition 4.1.1 that $s'_i \,|\, s'_{i+1}$ for $1 \leq i < (r-1)$. Furthermore, since $f_1 = \gcd(d, s'_1)$, it implies $f_1 \,|\, s'_1$, which further implies $f_1 \,|\, s'_2$ since $s'_1 \,|\, s'_2$. More generally, $f_1 \,|\, s'_i$ for all $i = 1, \ldots, r-1$, since $s'_i \,|\, s'_{i+1}$ for $1 \leq i < (r-1)$. Therefore, the nonzero diagonal entries $s''_1, s'_2, \ldots, s'_{r-1}$ of the submatrix B' of matrix A_3 are all divisible by f_1, and consequently, the nonzero diagonal entries $f_2, f_3, \ldots, f_r$ of the submatrix S'' of matrix S are all divisible by f_1. In fact, since $S'' = PB'Q$ is a diagonal matrix, if $P = (p_{ij})$, $Q = (q_{ij})$, $S'' = (s''_{ij})$, and $B' = (b'_{ij})$, then

$$s''_{ii} = \sum_{k=1}^{m-1} \sum_{l=1}^{n-1} p_{ik}\, b'_{kl}\, q_{li} \;\; = \sum_{k=1}^{\min\{m-1,n-1\}} p_{ik}\, b'_{kk}\, q_{ki}\,,$$

by matrix multiplication. Since $f_1 \,|\, b'_{kk}$ (i.e. $b'_{kk} = f_1 c_{kk}$ for some $c_{kk} \in \mathbb{F}[x]$) for $1 \leq k \leq (r-1)$, and $s''_{ii} = f_{i+1}$ for $1 \leq i \leq (r-1)$, we finally obtain

$$f_{i+1} = \sum_{k=1}^{r-1} p_{ik}\, b'_{kk}\, q_{ki} = \sum_{k=1}^{r-1} p_{ik}\, f_1 c_{kk}\, q_{ki} = f_1 \sum_{k=1}^{r-1} p_{ik}\, c_{kk}\, q_{ki}, \quad 1 \leq i \leq (r-1),$$

showing indeed that f_1 is a divisor of all nonzero diagonal entries $f_2, f_3, \ldots, f_r$ of the submatrix S'' of matrix S. In particular, f_1 divides f_2. Therefore, the matrix S is indeed in Smith normal form. Taking matrix U as the product of (invertible) matrices U_4, U_3, U_2 and U_1, i.e. $U = U_4U_3U_2U_1$, and matrix V as the product of (invertible) matrices V_1, V_2, V_3 and V_4, i.e. $V = V_1V_2V_3V_4$, then $UAV = S$. □

The matrix S in the Theorem 4.1.3 is in fact unique, and in order to prove this uniqueness, we will first consider some necessary definitions and results. From Theorem 2.1.6 in Chapter 1

of this thesis, we know that if R is a principal ideal domain and S is a subset of R, containing at least one nonzero element, then $d = \gcd(S)$ if and only if $\langle d \rangle = \langle S \rangle$. This fact gives rise to the following definition.

Definition 4.1.4. [1, p. 205] Let A be an $m \times n$ matrix over $\mathbb{F}[x]$, and $d_k(A)$ $(1 \leq k \leq \min\{m, n\})$ be the greatest common divisor (GCD) of $M_k(A)$, the set of all $k \times k$ minors of A, i.e. $d_k(A) = \gcd\big(M_k(A)\big)$. Then

$$DI_k(A) = \big\langle M_k(A) \big\rangle = \big\langle d_k(A) \big\rangle \subseteq \mathbb{F}[x],$$

where $DI_k(A)$ is the k-th determinantal ideal of A. A generator of $DI_k(A)$ is called the ***k*-th determinantal divisor of *A***.

Corollary 4.1.5. *Let A be an $m \times n$ matrix over $\mathbb{F}[x]$, and $S = (s_{ij})$ be a Smith normal form of A with nonzero (monic) diagonal entries $s_{ii} = f_i$ where $1 \leq i \leq r$, for some $r = 1, \ldots, \min\{m, n\}$. Then*

$$f_1 = d_1(A), \quad f_2 = \frac{d_2(A)}{d_1(A)}, \quad \cdots, \quad f_r = \frac{d_r(A)}{d_{r-1}(A)}.$$

Proof. Suppose S is a Smith normal form of A. Then by Theorem 4.1.3, there exist $m \times m$ invertible matrix U over $\mathbb{F}[x]$ and $n \times n$ invertible matrix V over $\mathbb{F}[x]$ such that $UAV = S$. Both U and V are products of elementary operation matrices over $\mathbb{F}[x]$, and so from Remark 3.2.15, $DI_k(A) = DI_k(UAV) = DI_k(S)$, for $k = 1, \ldots, \min\{m, n\}$. The ideals $DI_k(A) \subseteq \mathbb{F}[x]$ and $DI_k(S) \subseteq \mathbb{F}[x]$ are principal ideals, since $\mathbb{F}[x]$ is a PID. Hence, by the equality $DI_k(A) = DI_k(S)$, the (monic) generator $d_k(A)$ of $DI_k(A)$ equals the (monic) generator $d_k(S)$ of $DI_k(S)$, i.e. $d_k(A) = d_k(S)$, for $1 \leq k \leq \min\{m, n\}$. Now, suppose $f_1, f_2, \ldots, f_r$ are nonzero (monic) diagonal entries of S, where $1 \leq r \leq \min\{m, n\}$. Then $d_k(S) = f_1 \cdots f_k$, for $1 \leq k \leq r$, implying $d_k(A) = f_1 \cdots f_k$, for $1 \leq k \leq r$. Therefore, we obtain

$$f_1 = d_1(A), \quad f_2 = \frac{d_2(A)}{d_1(A)}, \quad \cdots, \quad f_r = \frac{d_r(A)}{d_{r-1}(A)}.$$

This completes the proof. □

Definition 4.1.6. Let A be an $m \times n$ matrix over $\mathbb{F}[x]$, and $S = (s_{ij})$ be a Smith normal form of A with nonzero (monic) diagonal entries $s_{ii} = f_i$ where $1 \leq i \leq r$, for some $r = 1, \ldots, \min\{m, n\}$. Each diagonal entry f_i, obtained in Corollary 4.1.5, is called the ***i*-th invariant factor of *A***, for $1 \leq i \leq r$.

Theorem 4.1.7. *[12, p. 260] Let A be a nonzero $m \times n$ matrix over $\mathbb{F}[x]$, and S be a Smith normal form of A. Then S is unique.*

Proof. A very short version of the proof of this result is given in [12] (Corollary, p. 260), however; a very concise proof is given here. Let $m \times n$ matrices $S = (s_{ij})$ and $T = (t_{ij})$ be Smith normal form of matrix A, with (monic) nonzero diagonal entries $s_{ii} = f_i$ $(1 \leq i \leq r)$ and $t_{ii} = g_i$ $(1 \leq i \leq r')$, respectively, where $1 \leq r, r' \leq \min\{m, n\}$. From Corollary 4.1.5, we obtain

$$f_1 = d_1(A), \quad f_2 = \frac{d_2(A)}{d_1(A)}, \quad \cdots, \quad f_r = \frac{d_r(A)}{d_{r-1}(A)},$$

and

$$g_1 = d_1(A), \quad g_2 = \frac{d_2(A)}{d_1(A)}, \quad \cdots, \quad g_{r'} = \frac{d_{r'}(A)}{d_{r'-1}(A)}.$$

From Theorem 4.1.3, since S and T are Smith normal forms of A, there exist $m \times m$ invertible matrices U and P, and $n \times n$ invertible matrices V and Q, such that $UAV = S$ and $PAQ = T$. From Lemma 3.2.16, since matrices U, V, P and Q are products of elementary matrices, we obtain

$$D\text{-rank}(S) = D\text{-rank}(UAV) = D\text{-rank}(A) = D\text{-rank}(PAQ) = D\text{-rank}(T).$$

Since S is a diagonal matrix with nonzero (monic) diagonal entries $f_1, f_2, \ldots, f_r$, it implies r is the largest positive integer less than or equal to $\min\{m, n\}$ such that there is a nonzero $r \times r$ minor of S, i.e. the determinantal rank of S is $D\text{-rank}(S) = r$. Similarly, $D\text{-rank}(T) = r'$. Therefore,

$$r = D\text{-rank}(S) = D\text{-rank}(A) = D\text{-rank}(T) = r',$$

i.e. $r = r' = D\text{-rank}(A)$. Hence, the uniqueness. □

Definition 4.1.8. Let A be an $m \times n$ matrix over $\mathbb{F}[x]$. The $m \times n$ matrix S over $\mathbb{F}[x]$ in the Theorem 4.1.3 is called the **Smith normal form of A.**

Example 4.1.9. Let

$$A = (a_{ij}) = \begin{bmatrix} x+1 & 0 & 0 \\ 0 & (x+1)^2(x+2) & 0 \\ 0 & 0 & (x+1)^2(x+3) \end{bmatrix}$$

be a 3×3 matrix over $\mathbb{Q}[x]$, where $\mathbb{Q}$ is the field of rational numbers. The matrix A satisfies all properties of Definition 4.1.1, except for the divisibility property. Though a_{11} divides a_{22},

a_{22} does not divide a_{33}; thus a need for Lemma 4.1.2 to be applied to the submatrix

$$B = \begin{bmatrix} (x+1)^2(x+2) & 0 \\ 0 & (x+1)^2(x+3) \end{bmatrix}$$

of A. On application of this lemma on matrix B, we obtain

$$\begin{bmatrix} (x+1)^2 & 0 \\ 0 & (x+1)^2(x+2)(x+3) \end{bmatrix},$$

and so the matrix

$$S = \begin{bmatrix} x+1 & 0 & 0 \\ 0 & (x+1)^2 & 0 \\ 0 & 0 & (x+1)^2(x+2)(x+3) \end{bmatrix},$$

becomes the SNF of A. In the following, we make it more explicit how to obtain the SNF S of A, by repeated application of the division algorithm to arrive at the desired matrix S.

$$A = \begin{bmatrix} x+1 & 0 & 0 \\ 0 & (x+1)^2(x+2) & 0 \\ 0 & 0 & (x+1)^2(x+3) \end{bmatrix} \xrightarrow[U_1A=A_1]{U_1=\left[\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right]} A_1 = \begin{bmatrix} x+1 & 0 & 0 \\ 0 & (x+1)^2(x+2) & (x+1)^2(x+3) \\ 0 & 0 & (x+1)^2(x+3) \end{bmatrix}$$

$$A_1 = \begin{bmatrix} x+1 & 0 & 0 \\ 0 & (x+1)^2(x+2) & (x+1)^2(x+3) \\ 0 & 0 & (x+1)^2(x+3) \end{bmatrix} \xrightarrow[A_1V_1=A_2]{V_1=\left[\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{smallmatrix}\right]} A_2 = \begin{bmatrix} x+1 & 0 & 0 \\ 0 & (x+1)^2(x+2) & (x+1)^2 \\ 0 & 0 & (x+1)^2(x+3) \end{bmatrix}$$

$$A_2 = \begin{bmatrix} x+1 & 0 & 0 \\ 0 & (x+1)^2(x+2) & (x+1)^2 \\ 0 & 0 & (x+1)^2(x+3) \end{bmatrix} \xrightarrow[A_2V_2=A_3]{V_2=\left[\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{smallmatrix}\right]} A_3 = \begin{bmatrix} x+1 & 0 & 0 \\ 0 & (x+1)^2 & (x+1)^2(x+2) \\ 0 & (x+1)^2(x+3) & 0 \end{bmatrix}$$

$$A_3 = \begin{bmatrix} x+1 & 0 & 0 \\ 0 & (x+1)^2 & (x+1)^2(x+2) \\ 0 & (x+1)^2(x+3) & 0 \end{bmatrix} \xrightarrow[A_3V_3=A_4]{V_3=\left[\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & -(x+2) \\ 0 & 0 & 1 \end{smallmatrix}\right]} A_4 = \begin{bmatrix} x+1 & 0 & 0 \\ 0 & (x+1)^2 & 0 \\ 0 & (x+1)^2(x+3) & -(x+1)^2(x+2)(x+3) \end{bmatrix}$$

$$A_4 = \begin{bmatrix} x+1 & 0 & 0 \\ 0 & (x+1)^2 & 0 \\ 0 & (x+1)^2(x+3) & -(x+1)^2(x+2)(x+3) \end{bmatrix} \xrightarrow[U_2A_4=A_5]{U_2=\left[\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -(x+3) & 1 \end{smallmatrix}\right]} A_5 = \begin{bmatrix} x+1 & 0 & 0 \\ 0 & (x+1)^2 & 0 \\ 0 & 0 & -(x+1)^2(x+2)(x+3) \end{bmatrix}$$

$$A_5 = \begin{bmatrix} x+1 & 0 & 0 \\ 0 & (x+1)^2 & 0 \\ 0 & 0 & -(x+1)^2(x+2)(x+3) \end{bmatrix} \xrightarrow[U_3A_5=A_6]{U_3=\left[\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{smallmatrix}\right]} A_6 = \begin{bmatrix} x+1 & 0 & 0 \\ 0 & (x+1)^2 & 0 \\ 0 & 0 & (x+1)^2(x+2)(x+3) \end{bmatrix}$$

Setting

$$U := U_3U_2U_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & x+3 & x+2 \end{bmatrix}, \qquad V := V_1V_2V_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & x+3 \\ 0 & 1 & -(x+2) \end{bmatrix},$$

and

$$S := A_6 = \begin{bmatrix} x+1 & 0 & 0 \\ 0 & (x+1)^2 & 0 \\ 0 & 0 & (x+1)^2(x+2)(x+3) \end{bmatrix},$$

then $UAV = S$. In other words, the matrix S is the Smith normal form of matrix A.

4.2 Partial Smith form of a polynomial matrix

Let A be an $m \times n$ matrix over the polynomial ring $\mathbb{F}[x_1, \ldots, x_k]$, $k \geq 2$. In this section, we assume the matrix A has many nonzero scalars (nonzero elements in $\mathbb{F}$) as entries. Allowing both elementary row and column operations, any nonzero scalar entry in A can be moved to the main diagonal, and then rescaled to become a leading 1; thereby becoming a pivot. All entries below this pivot (the leading 1) can then be reduced to zero using elementary row operations, and also all entries to the right of the pivot can be reduced to zero using elementary column operations. Performing this sequence of elementary row and column operations for each nonzero scalar entry in A, we obtain an $m \times n$ matrix

$$P = \left[\begin{array}{cccc|cccc} 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 & \cdots & 0 \\ \hline 0 & 0 & \cdots & 0 & * & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & * & * & \cdots & * \end{array}\right] = \left[\begin{array}{c|c} I_r & O_{r,n-r} \\ \hline O_{m-r,r} & B_{m-r,n-r} \end{array}\right]$$

over $\mathbb{F}[x_1, \ldots, x_k]$, where I_r is the $r \times r$ identity matrix, $B_{m-r,n-r}$ is an $(m-r) \times (n-r)$ matrix with no nonzero scalar entries, and $O_{r,n-r}$ and $O_{m-r,r}$ are $r \times (n-r)$ and $(m-r) \times r$ zero matrices respectively. Since only elementary (row and column) operations are performed on the matrix A in order to obtain the matrix P, there exists some $m \times m$ invertible matrix U over $\mathbb{F}[x_1, \ldots, x_k]$ and some $n \times n$ invertible matrix V over $\mathbb{F}[x_1, \ldots, x_k]$ such that $UAV = P$. The matrix U (resp. matrix V) is a product of some elementary row (resp. column) operation matrices over $\mathbb{F}[x_1, \ldots, x_k]$, and hence, invertible over $\mathbb{F}[x_1, \ldots, x_k]$, i.e. $\det(U)$ (resp. $\det(V)$) belongs to $\mathbb{F}\backslash\{0\}$. The primary reference in this subsection is [3] (Chapter 8, Section 4).

Definition 4.2.1. Let A be an $m \times n$ matrix over $\mathbb{F}[x_1, \ldots, x_k]$, $k \geq 2$. An $m \times n$ block

diagonal matrix

$$P = \left[\begin{array}{c|c} I_r & \\ \hline & B_{m-r,n-r} \end{array}\right]$$

over $\mathbb{F}[x_1, \ldots, x_k]$, consisting of an $r \times r$ identity matrix I_r and a lower right block $(m-r) \times (n-r)$ matrix $B_{m-r,n-r}$ which has no nonzero scalar entries, is called a **partial Smith form** of the original matrix A if $P = UAV$ for some invertible matrices U and V.

An algorithm for computing a partial Smith form of a matrix over $\mathbb{F}[x_1, \ldots, x_k]$, $k \geq 2$, will be given in Figure 4.1. This algorithm is the same as Algorithm 8.4.2.3 in [3], except that some notations are changed.

Example 4.2.2. Let

$$A = \begin{bmatrix} 1 & x_1 & x_2 & x_3 & x_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & x_1 & 0 & 0 & x_2 & 0 & x_3 & x_4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & x_1 & 0 & 0 & x_2 & 0 & 0 & x_3 & 0 & x_4 & 0 & 0 \\ 0 & 0 & 1 & 0 & x_1 & 0 & 0 & x_2 & 0 & 0 & x_3 & 0 & x_4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & x_1 & 0 & x_2 & 0 & 0 & x_3 & 0 & x_4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & x_1 & x_2 & x_3 & x_4 \end{bmatrix}$$

be a 6×14 matrix over $\mathbb{F}[x_1, x_2, x_3, x_4]$. A partial Smith form of matrix A is obtained as follows:

$$\begin{bmatrix} \mathbf{1} & x_1 & x_2 & x_3 & x_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & x_1 & 0 & 0 & x_2 & 0 & x_3 & x_4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & x_1 & 0 & 0 & x_2 & 0 & 0 & x_3 & 0 & x_4 & 0 & 0 \\ 0 & 0 & 1 & 0 & x_1 & 0 & 0 & x_2 & 0 & 0 & x_3 & 0 & x_4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & x_1 & 0 & x_2 & 0 & 0 & x_3 & 0 & x_4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & x_1 & x_2 & x_3 & x_4 \end{bmatrix}$$

$$\longrightarrow \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -x_1 & -x_2 + x_1 & -x_3 & -x_4 & x_2 & 0 & x_3 & x_4 & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & x_1 & 0 & 0 & x_2 & 0 & 0 & x_3 & 0 & x_4 & 0 & 0 \\ 0 & 0 & 1 & 0 & x_1 & 0 & 0 & x_2 & 0 & 0 & x_3 & 0 & x_4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & x_1 & 0 & x_2 & 0 & 0 & x_3 & 0 & x_4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & x_1 & x_2 & x_3 & x_4 \end{bmatrix}$$

Input: An $m \times n$ matrix A with entries in $\mathbb{F}[x_1, \ldots, x_k]$.

Output: The quantities P, r, B where P is an $m \times n$ block diagonal matrix $P = \mathrm{diag}(I_r, B)$ consisting of an identity matrix of size r and a lower right block $B = B_{m-r,n-r}$ in which no entry is a nonzero scalar.

Initialization: Set $P \leftarrow A$. Set $l \leftarrow 1$.

- While $p_{ij} \in \mathbb{F}\backslash\{0\}$ for some $i, j \geq l$ do:
  - Find the least $i \geq l$ for which $p_{ij} \in \mathbb{F}\backslash\{0\}$ for some $j \geq l$.
  - If $i \neq l$, then interchange rows i and l of P.
  - Find the least $j \geq l$ for which $p_{lj} \in \mathbb{F}\backslash\{0\}$.
  - If $j \neq l$, then interchange columns j and l of P.
  - If $p_{ll} \neq 1$, then divide row l of P by p_{ll}.
  - For $i = l+1, \ldots, m$ do: subtract p_{il} times row l from row i.
  - For $j = l+1, \ldots, n$ do: subtract p_{lj} times column l from column j.
  - Set $l \leftarrow l + 1$.
- Set $r \leftarrow l - 1$
- Set $B \leftarrow P(r+1, \ldots, m; r+1, \ldots, n)$, which is the $(m-r) \times (n-r)$ submatrix of P consisting of entries whose row indices are in $\{r+1, \ldots, m\}$ and column indices are in $\{r+1, \ldots, n\}$
- Return P, r, B.

Figure 4.1: Partial Smith form

$$\longrightarrow \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & x_1 & 0 & 0 & x_2 & 0 & 0 & x_3 & 0 & x_4 & 0 & 0 \\ 0 & -x_1 & -x_2+x_1 & -x_3 & -x_4 & x_2 & 0 & x_3 & x_4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & x_1 & 0 & 0 & x_2 & 0 & 0 & x_3 & 0 & x_4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & x_1 & 0 & x_2 & 0 & 0 & x_3 & 0 & x_4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & x_1 & x_2 & x_3 & x_4 \end{bmatrix}$$

$$\longrightarrow \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -x_2+x_1 & x_1^2-x_3 & -x_4 & x_2 & x_1x_2 & x_3 & x_4 & x_1x_3 & 0 & x_1x_4 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & x_1 & 0 & 0 & x_2 & 0 & 0 & x_3 & 0 & x_4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & x_1 & 0 & x_2 & 0 & 0 & x_3 & 0 & x_4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & x_1 & x_2 & x_3 & x_4 \end{bmatrix}$$

$$\longrightarrow \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & x_1^2-x_3 & x_1x_2-x_1^2-x_4 & x_2 & x_1x_2 & x_2^2-x_1x_2+x_3 & x_4 & x_1x_3 & x_2x_3-x_1x_3 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} & x_1 & 0 & x_2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & x_1 \end{bmatrix}$$

$$\begin{matrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ x_1x_4 & x_2x_4-x_1x_4 & 0 \\ x_3 & 0 & x_4 \\ x_2 & x_3 & x_4 \end{bmatrix}$$

$$\longrightarrow \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & x_1x_2-x_1^2-x_4 & x_1^2-x_3 & 0 & x_2^2-x_1x_2+x_3 & -x_2^2+x_4 & x_1x_3 & x_2x_3-x_1x_3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & x_1 \end{bmatrix}$$

$$\left[\begin{array}{ccc}
0 & 0 & 0 \\
0 & 0 & 0 \\
0 & 0 & 0 \\
0 & 0 & 0 \\
-x_2x_3+x_1x_4 & x_2x_4-x_1x_4 & -x_2x_4 \\
x_2 & x_3 & x_4
\end{array}\right]$$

$$\longrightarrow \left[\begin{array}{ccccc|ccccccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & 0 & 0 & x_1^2-x_3 & 0 & x_2^2-x_1x_2+x_3 & -x_2^2+x_4 & x_1x_2-x_1^2-x_4 & -x_1^2x_3+x_2x_3-x_1x_3
\end{array}\right].$$

$$\left[\begin{array}{ccc}
0 & 0 & 0 \\
0 & 0 & 0 \\
0 & 0 & 0 \\
0 & 0 & 0 \\
0 & 0 & 0 \\
\hline
-x_1x_2x_3-x_2x_3+x_1x_4 & -x_1x_3^2-x_1x_4+x_2x_4 & -x_1x_3x_4-x_2x_4
\end{array}\right].$$

The matrix

$$P = \left[\begin{array}{c|c} I_5 & O_{5,9} \\ \hline O_{1,5} & B_{1,9} \end{array}\right]$$

is a partial Smith form of matrix A, where $B_{1,9}$ is the 1×9 matrix

$$B^t = \left[\begin{array}{c}
x_1^2-x_3 \\
0 \\
x_2^2-x_1x_2+x_3 \\
-x_2^2+x_4 \\
x_1x_2-x_1^2-x_4 \\
-x_1^2x_3+x_2x_3-x_1x_3 \\
-x_1x_2x_3-x_2x_3+x_1x_4 \\
-x_1x_3^2-x_1x_4+x_2x_4 \\
-x_1x_3x_4-x_2x_4
\end{array}\right].$$

From the above example, the indeterminates x_1, x_2, x_3, x_4 can be regarded as variables, where values from the field $\mathbb{F}$ can be assigned to them. If this is the case, then the original matrix A will be a matrix over the field $\mathbb{F}$, and so from its partial Smith form P, it will have a rank ≥ 5. In particular, if submatrix B of P is a zero matrix, then $\text{rank}\,(A) = 5$. An interesting question to ask is: what are the values of x_1, x_2, x_3, x_4 (if any) that will give $B = 0$? This is equivalent to solving for common zeroes of the polynomial entries in B.

In general, given a matrix A over $\mathbb{F}[x_1, \ldots, x_k]$, $k \geq 2$, with many nonzero scalars as entries, a partial Smith form $P = \text{diag}\big(I_r, B_{m-r,n-r}\big)$ of A can be obtained. The original matrix A will have rank exactly equal to r, provided the matrix $B_{m-r,n-r}$ is a zero matrix. In order to know the values of the variables $x_1, \ldots, x_k$ that will make matrix B become zero, it suffices to solve for common zeroes of the (polynomial) entries in B. However, solving in general for common zeroes of some finite polynomials $f_1, \ldots, f_n$ can be somewhat difficult. Obtaining first a *simple* basis (set of generators) for the ideal $\langle f_1, \ldots, f_n \rangle$, generated by these finite polynomials $f_1, \ldots, f_n$, makes the computation for their common zeroes easier. In the next section, we will give an overview of obtaining simple bases for submodules of free R-modules R^n, where $R = \mathbb{F}[x_1, \ldots, x_k]$. A special case of this is when $n = 1$, which is just the theory of obtaining Gröbner bases for ideals of polynomial rings $\mathbb{F}[x_1, \ldots, x_k]$.

4.3 Gröbner bases for submodules of R^n, $n \geq 1$, $R = \mathbb{F}[x_1, \ldots, x_k]$

Throughout this section, R will still stand for the polynomial ring $\mathbb{F}[x_1, \ldots, x_k]$, where $\mathbb{F}$ is a field. Also, $\{e_1, \ldots, e_n\}$ will stand for the standard (ordered) basis in the free R-module R^n. The primary references, here in this subsection, are [7] and [8].

4.3.1 Monomial orderings in R^n

Definition 4.3.1. A **monomial** in R^n is a vector of the form $x^\alpha e_i = \big(0, \ldots, 0, x^\alpha, 0, \ldots, 0\big)^T$, where $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_k^{\alpha_k}$, is in the i-th position of the vector, for some i, $1 \leq i \leq k$, and each α_j, $1 \leq j \leq k$ is a non-negative integer.

Definition 4.3.2. A **monomial ordering** on R^n is a relation $>$ that satisfies the following conditions:

i. $>$ is a (strict) total ordering; that is, it satisfies:

- Transitivity: For all monomials $x^\alpha e_{i_1}, x^\beta e_{i_2}, x^\gamma e_{i_3}$ in R^n, we have:

$$x^\alpha e_{i_1} > x^\beta e_{i_2}, \quad x^\beta e_{i_2} > x^\gamma e_{i_3} \quad \Longrightarrow \quad x^\alpha e_{i_1} > x^\gamma e_{i_3}.$$

- Trichotomy: For all $x^\alpha e_i, x^\beta e_j$ in R^n, exactly one of the following holds:

$$x^\alpha e_i > x^\beta e_j, \qquad x^\beta e_j > x^\alpha e_i, \qquad x^\alpha e_i = x^\beta e_j.$$

ii. For any monomials $x^\alpha e_i$ and $x^\beta e_j$ in R^m with $x^\alpha e_i > x^\beta e_j$, we have $x^\gamma x^\alpha e_i > x^\gamma x^\beta e_j$, for all $x^\gamma \in R$.

iii. $>$ is a well ordering, i.e. every nonempty set containing monomials in R^n has a least element with respect to $>$.

Remark 4.3.3. Trichotomy implies both antisymmetry and totality. *Antisymmetry:* If we define the negation of the relation $>$ as usual by $x^\alpha e_i \leq x^\beta e_j \iff \text{not}(x^\alpha e_i > x^\beta e_j)$, then $x^\alpha e_i \leq x^\beta e_j$ and $x^\beta e_j \leq x^\alpha e_i$ imply $x^\alpha e_i = x^\beta e_j$. (If the first two parts of trichotomy are false, then the third must be true.) *Totality:* Trichotomy says that $x^\alpha e_i > x^\beta e_j$ or $x^\alpha e_i = x^\beta e_j$ or $x^\beta e_j > x^\alpha e_i$. Trivially, the statement P: $x^\alpha e_i = x^\beta e_j$ is equivalent to the redundant disjunction P or P. Therefore trichotomy is equivalent to the statements $x^\alpha e_i > x^\beta e_j$ or $x^\alpha e_i = x^\beta e_j$, or $x^\beta e_j > x^\alpha e_i$ or $x^\beta e_j = x^\alpha e_i$. These disjunctions can be more concisely written as: $\text{not}(x^\beta e_j > x^\alpha e_i)$, or $\text{not}(x^\alpha e_i > x^\beta e_j)$. But this last disjunction is exactly the totality property: $x^\alpha e_i \leq x^\beta e_j$ or $x^\beta e_j \leq x^\alpha e_i$.

There are many monomial orderings on the set of monomials in R. Some common examples are given below.

Example 4.3.4.

a. Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n)$ be n-tuples of positive integers. Then, $x^\alpha >_{\text{lex}} x^\beta$, if in the vector difference $\alpha - \beta \in \mathbb{Z}$, the leftmost nonzero entry is positive. This kind of ordering is called a **lexicographic ordering**, denoted **lex**.

b. Other common examples are reverse lexicographic ordering, degree reverse lexicographic ordering, etc.

Given a monomial order $>$ on set of monomials in R, there are two natural ways of extending this monomial order to monomial order in R^n. These two ways are given in the next definition.

Definition 4.3.5. Let $>$ be a monomial ordering on R.

i. For monomials $x^\alpha e_i$ and $x^\beta e_j$ in R^n, we say that $x^\alpha e_i \geq_{\text{TOP}} x^\beta e_j$ if and only if $x^\alpha > x^\beta$ or $x^\alpha = x^\beta$ and $i \leq j$.

ii. For monomials $x^\alpha e_i$ and $x^\beta e_j$ in R^n, we say that $x^\alpha e_i \geq_{\text{POT}} x^\beta e_j$ if and only if $i < j$ or $i = j$ and $x^\alpha \geq x^\beta$.

Remark 4.3.6. In the above definition, TOP stands for *term over position*, and POT stands for *position over term*. While the TOP ordering sorts monomials in R^n first by their term order on R and then uses their positions (coordinate position as a vector in R^n) if there are any ties, the POT ordering does the reverse. Also, in the above definition, it has been assumed that the standard basis vectors $e_1, \ldots, e_n$, are ordered as $e_1 > e_2 > \cdots > e_n$, and this particular ordering is called a **downward ordering** on $\{e_1, \ldots, e_n\}$ in [8]. The analogue, $e_n > e_{n-1} > \cdots > e_1$ can also be assumed, and this gives a slight change to Definition 4.3.5; more precisely, every appearance of $i < j$ (resp. $i \leq j$) will be replaced by $j < i$ (resp. $j \leq i$).

It will soon be shown that for any monomial order $>$ on R, the two orderings given in Definition 4.3.5 truly define monomial orderings on R^n. In order to achieve this, some important results will first be given – these results will help in showing easily that both orderings **POT** and **TOP** on R^n are well ordering. But before that, a simple example will be given to explain how Definition 4.3.5 works.

Example 4.3.7. Assume $e_1 > e_2$.

i. If the lexicographic ordering, **lex** (Example 4.3.4 (a)) on $\mathbb{Q}[x, y]$ with $x > y$ is extended to a **TOP** ordering on $\mathbb{Q}[x, y]^2$, then the monomials $(x^3y, 0)^T$, $(y^3, 0)^T$, $(x, 0)^T$, $(0, x^4)^T$,

$(0, xy^2)^T$, $(0, x)^T$, $(0, y^2)^T$ in $\mathbb{Q}[x, y]^2$ are ordered as follows:

$$\begin{pmatrix} 0 \\ x^4 \end{pmatrix} >_{\text{TOP}} \begin{pmatrix} x^3y \\ 0 \end{pmatrix} >_{\text{TOP}} \begin{pmatrix} 0 \\ xy^2 \end{pmatrix} >_{\text{TOP}} \begin{pmatrix} x \\ 0 \end{pmatrix} >_{\text{TOP}} \begin{pmatrix} 0 \\ x \end{pmatrix} >_{\text{TOP}} \begin{pmatrix} y^3 \\ 0 \end{pmatrix} >_{\text{TOP}} \begin{pmatrix} 0 \\ y^2 \end{pmatrix}.$$

ii. If the same lexicographic ordering, **lex** on $\mathbb{Q}[x, y]$ with $x > y$ is extended to a **POT** ordering on $\mathbb{Q}[x, y]^2$, then the same monomials in part (i) above are ordered as follows:

$$\begin{pmatrix} x^3y \\ 0 \end{pmatrix} >_{\text{POT}} \begin{pmatrix} x \\ 0 \end{pmatrix} >_{\text{POT}} \begin{pmatrix} y^3 \\ 0 \end{pmatrix} >_{\text{POT}} \begin{pmatrix} 0 \\ x^4 \end{pmatrix} >_{\text{POT}} \begin{pmatrix} 0 \\ xy^2 \end{pmatrix} >_{\text{POT}} \begin{pmatrix} 0 \\ x \end{pmatrix} >_{\text{POT}} \begin{pmatrix} 0 \\ y^2 \end{pmatrix}.$$

Every nonzero element f in R^n can be written as a finite linear combination, with nonzero coefficients in $\mathbb{F}$, of monomials in R^n. For example, the nonzero element

$$f = (2x^3y - y^3 + 5x, -6x^4 + 3xy^2 + 4x + y^2)^T$$

in $\mathbb{Q}[x, y]^2$ is written as:

$$\begin{aligned} f &= 2\begin{pmatrix} x^3y \\ 0 \end{pmatrix} - \begin{pmatrix} y^3 \\ 0 \end{pmatrix} + 5\begin{pmatrix} x \\ 0 \end{pmatrix} - 6\begin{pmatrix} 0 \\ x^4 \end{pmatrix} + 3\begin{pmatrix} 0 \\ xy^2 \end{pmatrix} + 4\begin{pmatrix} 0 \\ x \end{pmatrix} + \begin{pmatrix} 0 \\ y^2 \end{pmatrix} \\ &= 2x^3ye_1 - y^3e_1 + 5xe_1 - 6x^4e_2 + 3xy^2e_2 + 4xe_2 + y^2e_2. \end{aligned} \tag{4.1}$$

Now, using the monomial ordering **TOP** given in Example 4.3.7 (i), the element f in $\mathbb{Q}[x, y]^2$ as in (4.1) is rewritten as $f = -6x^4e_2 + 2x^3ye_1 + 3xy^2e_2 + 5xe_1 + 4xe_2 - y^3e_1 + y^2e_2$, in descending order of monomials of f. The leading coefficient, leading monomial and leading term of f are -6, x^4e_1 and $-6x^4e_1$, respectively. However, using the monomial ordering **POT** given in Example 4.3.7 (ii), the element $f \in \mathbb{Q}[x, y]^2$ as in (4.1) is now rewritten as $f = 2x^3ye_1 + 5xe_1 - y^3e_1 - 6x^4e_2 + 3xy^2e_2 + 4xe_2 + y^2e_2$, in descending order of monomials of f. The leading coefficient, leading monomial and leading term of f are now 2, x^3ye_1 and $2x^3ye_1$, respectively.

Proposition 4.3.13 demonstrates that any monomial submodule of R^n is finitely generated and any ascending chain of monomial submodules of R^n eventually terminates. Before this result is stated and proved, some terms need to be defined.

Definition 4.3.8. A submodule $M \subseteq R^n$ is a **monomial submodule** if M can be generated by a collection of monomials.

Definition 4.3.9. Let $x^\alpha e_i$ and $x^\beta e_j$ be any two monomials in R^n. Then $x^\alpha e_i$ is **divisible** by $x^\beta e_j$ (or $x^\beta e_j$ divides $x^\alpha e_i$) provided i equals j and $x^\alpha = x^\gamma x^\beta$, for some $x^\gamma \in R$. If $X = x^\alpha e_i$ is divisible by $Y = x^\beta e_j$, the **quotient** X/Y is an element of the ring R and equals $x^\alpha / x^\beta = x^{\alpha-\beta} = x^\gamma$.

Definition 4.3.10. Let $x^\alpha e_i$ and $x^\beta e_j$ be any two monomials in R^n. If $i = j$, the **greatest common divisor** of $x^\alpha e_i$ and $x^\beta e_j$, denoted $\gcd\left(x^\alpha e_i, x^\beta e_j\right)$, is the greatest common divisor of x^α and x^β, times e_i, i.e. $\gcd\left(x^\alpha e_i, x^\beta e_j\right) = \gcd\left(x^\alpha, x^\beta\right) e_i$.

Definition 4.3.11. Let $x^\alpha e_i$ and $x^\beta e_j$ be any two monomials in R^n. If $i = j$, the **least common multiple** of $x^\alpha e_i$ and $x^\beta e_j$, denoted $\operatorname{lcm}\left(x^\alpha e_i, x^\beta e_j\right)$, is the least common multiple of x^α and x^β, times e_i. Otherwise, $\operatorname{lcm}\left(x^\alpha e_i, x^\beta e_j\right) = 0$, i.e. whenever $i \neq j$.

The first part of the next proposition demonstrates that every monomial submodule M of R^n is finitely generated. Its second part guarantees that an infinite ascending chain of monomial submodules of R^n will eventually terminate. Dickson's Lemma (stated below without proof) plays a major role in the proof of the first part. The proof of the proposition follows the same argument given in [8] (Proposition 2.3, Chapter 5), though more details are given here.

Lemma 4.3.12 (Dickson's Lemma)**.** *Let A be a subset of $\mathbb{Z}^k_{\geq 0}$ and $I = \langle x^\alpha : \alpha \in A \rangle \subseteq R$ be a monomial ideal. Then, I is finitely generated as a monomial ideal, i.e. I can be written in the form $I = \left\langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \right\rangle$, where $x^{\alpha(1)}, \ldots, x^{\alpha(s)} \in A$.*

Proof. Proof of Theorem 5 in Chapter 4 of [7]. □

Proposition 4.3.13.

a. Every monomial submodule of R^n is generated by a finite collection of monomials.

b. Every infinite ascending chain $M_1 \subseteq M_2 \subseteq \cdots$ of monomial submodules of R^n stabilizes. That is, there exists N_0 such that $M_N = M_{N_0}$ for all $N \geq N_0$.

Proof.

a. Let M be a monomial submodule of R^n. For each i, $1 \leq i \leq n$, let $M_i = M \cap Re_i$ be subset of M consisting of elements whose jth components are zero for all $j \neq i$. For a

fixed i, $1 \leq i \leq n$, let X_1, X_2 be elements in M_i and r be any polynomial in R. The jth components of $rX_1 - X_2$ are zero for all $j \neq i$. Also, since M is a submodule of R^n, $rX_1 - X_2$ belongs to M, and thus, $rX_1 - X_2$ is in M_i, i.e. M_i is an R-submodule of M.

Every element of M_i (i being fixed) is of the form fe_i for some $f \in R$, and so M_i equals $I_i e_i$ for some ideal $I_i \subseteq R$. Since elements in M_i are also in M, this implies I_i is a monomial ideal in R and thus I_i is finitely generated by Lemma 4.3.12, i.e. I_i is a finitely generated monomial ideal in R. Therefore, M_i is a finitely generated monomial submodule of M, i.e. there exists monomials $x^{\alpha(i1)}, x^{\alpha(i2)}, \ldots, x^{\alpha(id_i)}$ in R such that $M_i = \left\langle x^{\alpha(i1)}, \ldots, x^{\alpha(id_i)} \right\rangle e_i$. Hence,

$$M = \left\langle \left\{ x^{\alpha(ij)} e_i \right\}_{\substack{1 \leq i \leq n \\ 1 \leq j \leq d_i}} \right\rangle.$$

b. Considering $M = \bigcup_{i=1}^{\infty} M_i$, it will be shown that M is also a monomial submodule of R^n, given that each M_i, $i \geq 1$ is a monomial submodule of R^n. First, the zero element in R^n belongs to M, since $0 \in M_i$ for each i, and M is a union (infinite) of M_i, $i \geq 1$. Now, let X_1, X_2 be any elements in M. Then X_1 and X_2 belong to M_i and M_j, respectively for some $i, j \geq 1$. Assuming $i \leq j$, then M_i is contained in M_j by the ascending chain $M_1 \subseteq M_2 \subseteq \cdots$. Thus, X_1 belongs to M_j, and also rX_1 belongs to M_j for all $r \in R$, since M_j is a submodule of R^n. Furthermore, $rX_1 - X_2$ belongs to M_j, the reason being that both rX_1 and $-X_2$ are in M_j, M_j being a submodule of R^n. Therefore, $rX_1 - X_2$ belongs to M, since M_j is contained in M, i.e. M is also a submodule (monomial) of R^n. By part (a) of this proposition, M is generated by a finite collection of monomials, i.e. $M = \langle X_1, X_2, \ldots, X_m \rangle$, $m \geq 1$. For each j, $1 \leq j \leq m$, X_j belongs to M_{i_j} for some $i_j \geq 1$. Setting $N_0 := \max_{1 \leq j \leq m} \{i_j\}$, then X_j belongs to M_{N_0} for all j, $1 \leq j \leq m$. Therefore,

$$\bigcup_{i=1}^{\infty} M_i = M = \langle X_1, X_2, \ldots, X_m \rangle \subseteq M_{N_0} \subseteq M_{N_0+1} \subseteq \ldots \subseteq \bigcup_{i=1}^{\infty} M_i,$$

i.e.

$$M = \bigcup_{i=1}^{\infty} M_i \subseteq M_{N_0} \subseteq M_{N_0+1} \subseteq \ldots \subseteq \bigcup_{i=1}^{\infty} M_i = M,$$

implying $M_N = M_{N_0}$ for all $N \geq N_0$, as required.

This completes the proof. □

Proposition 4.3.13 helps in proving the next result which is an equivalent statement to the well ordering property of Definition 4.3.2.

Proposition 4.3.14. *Let $>$ be a relation on the monomials of R^n satisfying conditions (i) and (ii) of Definition 4.3.2. Then $>$ is a well ordering on the monomials of R^n if and only if $x^\alpha X > X$ for all monomials $X \in R^n$ and all monomials $x^\alpha \in R$ with $x^\alpha \neq 1$.*

Proof. Let $>$ be a well ordering on the monomials of R^n and x^α be any monomial in R different from 1 (i.e. $x^\alpha \neq 1$), i.e. $x^\alpha X \neq X$ for any monomial $X \in R^n$. Then by condition (i) of Definition 4.3.2, either $x^\alpha X > X$ or $X > x^\alpha X$. Suppose $X > x^\alpha X$. Then by condition (ii) of Definition 4.3.2, $x^\alpha X > x^\alpha x^\alpha X$, i.e. $x^\alpha X > x^{2\alpha} X$. Similarly, from the last relation, using again condition (ii) of Definition 4.3.2, we obtain $x^{2\alpha} X > x^{3\alpha} X$. Continuing this way, we obtain a nonempty subset $\{X, x^\alpha X, x^{2\alpha} X, x^{3\alpha} X, \ldots\}$ of monomials in R^n with no least element, a contradiction to the assumption that $>$ is a well ordering on the monomials of R^n. Hence, $x^\alpha X > X$.

Conversely, suppose $x^\alpha X > X$ for all monomials $X \in R^n$ and for all monomials $x^\alpha \in R$ with $x^\alpha \neq 1$. Let S be any nonempty subset of the monomials of R^n. Then it will be shown that S has a least element. To this end, set $M := \langle S \rangle$, the monomial submodule generated by S. By Proposition 4.3.13(a), M is finitely generated by a finite collection of monomials in S, say X_i, $1 \leq i \leq r$. By condition (i) of Definition 4.3.2, these monomials generating M can be relabeled (if necessary) such that $X_r > \cdots > X_2 > X_1$. Having done this, it can be shown that the monomial X_1 is the least element of S with respect to $>$, i.e. $Y > X_1$, for all monomials $Y \in S$ different from X_i, $1 \leq i \leq r$. To see this, let Y be any monomial in S different from X_i, for all i, $1 \leq i \leq r$. Y belongs to M, and so is divisible by some X_i, $1 \leq i \leq r$. That is, there exists $x^\beta \in R$ such that $Y = x^\beta X_i$ for some i, $1 \leq i \leq r$ ($x^\beta \neq 1$, since $Y \neq X_i$ for all i, $1 \leq i \leq r$). Thus, by the above hypothesis ($x^\alpha X > X$ for all monomials $X \in R^m$ and for all monomials $x^\alpha \in R$ with $x^\alpha \neq 1$), $x^\beta X_i > X_i$ for all i, $1 \leq i \leq r$, and so $Y = x^\beta X_i > X_i \geq X_1$, for all i, $1 \leq 1 \leq r$. □

It will now be verified that the TOP ordering defined in Definition 4.3.5 (i) is indeed a monomial ordering on R^n. First, that $\geq_{\text{TOP}}$ is a total ordering on R^n follows from the facts that $>$ is a total ordering on R and the relation *less than or equal to,* $\leq$ is a total ordering

on any subset of set of natural numbers. Let $x^\alpha e_i$ and $x^\beta e_j$ be any monomials in R^n with $x^\alpha e_i \geq_{\text{TOP}} x^\beta e_j$. Then from definition of $\geq_{\text{TOP}}$, $x^\alpha > x^\beta$ or $x^\alpha = x^\beta$ and $i \leq j$, where $>$ is the monomial ordering on R and $\leq$ is a total ordering on $\{1, 2, \ldots, n\} \subset \mathbb{N}$. First, if $x^\alpha > x^\beta$, it implies by definition of monomial ordering on R that $x^\gamma x^\alpha > x^\gamma x^\beta$, for all $x^\gamma \in R$. And if $x^\alpha = x^\beta$, it first implies that $i \leq j$ (from definition of $\geq_{\text{TOP}}$) and then $x^\gamma x^\alpha = x^\gamma x^\beta$, for all $x^\gamma \in R$. Therefore, either $x^\gamma x^\alpha > x^\gamma x^\beta$ or $x^\gamma x^\alpha = x^\gamma x^\beta$ and $i \leq j$, i.e. $x^\gamma x^\alpha e_i \geq_{\text{TOP}} x^\gamma x^\beta e_j$. Finally, from Proposition 4.3.14, in order to show that $\geq_{\text{TOP}}$ is a well ordering on R^n, it suffices to show that $x^\alpha X \geq_{\text{TOP}} X$ for all monomials $X \in R^m$ and all monomials $x^\alpha \in R$ with $x^\alpha \neq 1$. But this is equivalent to showing that $x^\alpha > 1$ for all monomials $x^\alpha \in R$ with $x^\alpha \neq 1$, which is just the special case of Proposition 4.3.14 when $n = 1$. Hence, $\geq_{\text{TOP}}$ is a well ordering on the set of monomials in R^n. This completes the verification that the TOP ordering defined in Definition 4.3.5 (i) is indeed a monomial ordering on the set of monomials in R^n. The same argument can be used to show that the POT ordering defined in Definition 4.3.5 (ii) is also a monomial ordering on the set of monomials in R^n.

4.3.2 Division algorithm in R^n

In this subsection, an algorithm for computing a *remainder* when an element in R^n is divided by a finite set of elements in R^n, will be given. But before that, a result that leads to the algorithm will be considered. This result is called *division algorithm in* R^n, and its proof is exactly the same as the proof for the special case when $n = 1$.

Theorem 4.3.15. *Fix a monomial order $>$ on R^n, and let $F = (f_1, \ldots, f_s)$ be an ordered s-tuple of elements of R^n. Then every $f \in R^n$ can be written as*

$$f = \sum_{i=1}^{s} a_i f_i + r,$$

where $a_i \in R$, $r \in R^n$, $LT(a_i f_i) \geq LT(f)$ for all i, $1 \leq i \leq s$, and either $r = 0$ or r is a $\mathbb{F}$-linear combination of monomials, none of which is divisible by any of $LM(f_1), \ldots, LM(f_s)$.

Proof. The proof is exactly the same as the proof for the special case when $n = 1$, i.e. division algorithm in R (Theorem 3 in Section 3, Chapter 2 of [7]). There, an algorithm was given to show the existence of $a_1, \ldots, a_s$ and r. Except for monomial orderings, the same algorithm

can be used to show the existence of $a_1, \ldots, a_s$ and r in the general case. The termination of this algorithm in the general case follows from Proposition 4.3.14. □

Definition 4.3.16. The variable $r \in R^m$ in Theorem 4.3.15 is called a remainder of f on division by $F = (f_1, \ldots, f_s)$.

As said earlier, there is an algorithm for obtaining a remainder when an arbitrary element in R^n is divided by any finite set of elements in R^n. In fact, except for monomial orderings, this algorithm is the same as the algorithm for computing a remainder when an arbitrary polynomial in R is divided by any finite set of polynomials in R (i.e. a special case when $n = 1$). The algorithm for the case $n = 1$ is given in the proof of Theorem 3, Section 3, Chapter 2 of [7], and it will be reproduced in this subsection as *Division Algorithm in* R^n (Algorithm 4.2).

Example 4.3.17. Let $F = \{f_1 = (ab^2 + 1, a),\ f_2 = (a^2b + 1, b)\} \subseteq \mathbb{Q}[a, b]^2$ and $f = (a^3b - ab^3, a^2 - b^2)$ be an element of $\mathbb{Q}[a, b]^2$.

(a) Assume $e_1 > e_2$. If the lexicographic ordering, **lex** on $\mathbb{Q}[a, b]$, with $b \prec a$, is extended to a **TOP** ordering on $\mathbb{Q}[a, b]^2$, then dividing f by F, we obtain the following, where the leading term of each element in $\mathbb{Q}[a, b]^2$ is put in bold form:

$$
\begin{array}{rl}
 & -b \\
 & a \\
(\boldsymbol{ab^2} + 1,\ a) & \overline{\phantom{(\boldsymbol{a^3b} - ab^3,\ a^2 - b^2)}} \\
(\boldsymbol{a^2b} + 1,\ b) & \big| \ (\boldsymbol{a^3b} - ab^3,\ a^2 - b^2) \\
 & -\ (\boldsymbol{a^3b} + a,\ ab) \\
 & \overline{\phantom{(\boldsymbol{-ab^3} - a,\ a^2 - b^2 - ab)}} \\
 & -\ (\boldsymbol{-ab^3} - b,\ -ab) \\
 & \overline{\phantom{(-a + b,\ \boldsymbol{a^2} - b^2)}} \\
 & (\boldsymbol{-ab^3} - a,\ a^2 - b^2 - ab) \\
 & (-a + b,\ \boldsymbol{a^2} - b^2)
\end{array}
$$

That is,

$$f = -bf_1 + af_2 + (-a + b,\ a^2 - b^2),$$

with respect to the given orderings.

Input: $f, f_1, \ldots, f_s \in R^m$ with $f_i \neq 0$, $1 \leq i \leq s$

Output: $a_1, \ldots, a_s \in R = \mathbb{F}[X]$, $r \in R^m$ such that $f = \sum_{i=1}^{s} a_i f_i + r$ and either $r = 0$ or r is a $\mathbb{F}$-linear combination of monomials, none of which is divisible by any of $\mathrm{LM}(f_i)$, $1 \leq i \leq s$

Initialization: $a_i \leftarrow 0$ for all $i = 1, \ldots, s$, $r \leftarrow 0$, $p \leftarrow f$

WHILE $p \neq 0$ DO
    $i \leftarrow 1$
    division-occured $\leftarrow$ False

    WHILE $i \leq s$ and *division-occured* = False DO
        IF $\mathrm{LT}(f_i)$ divides $\mathrm{LT}(p)$ THEN
            $a_i = a_i + \mathrm{LT}(p) / \mathrm{LT}(f_i)$
            $p = p - (\mathrm{LT}(p) / \mathrm{LT}(f_i)) f_i$
            division-occured $\leftarrow$ True
        ELSE
            $i \leftarrow i + 1$
    IF *division-occured* = False THEN
        $r = r + \mathrm{LT}(p)$
        $p = p - \mathrm{LT}(p)$

Algorithm 4.2: Division algorithm in R^n

(b) Assume here $e_2 > e_1$. If the lexicographic ordering, **lex** on $\mathbb{Q}[a,b]$ with $b \prec a$ is extended to a **POT** ordering on $\mathbb{Q}[a,b]^2$, then dividing f by F, we obtain the following, where the leading term of each element in $\mathbb{Q}[a,b]^2$ is put in bold form:

$$\begin{array}{rl}
 & a \\
 & -b \\
\begin{matrix}(ab^2+1,\ \boldsymbol{a})\\ (a^2b+1,\ \boldsymbol{b})\end{matrix}\Big| & \overline{(a^3b-ab^3,\ \boldsymbol{a^2}-b^2)} \\
 & -\ \underline{(a^2b^2+a,\ \boldsymbol{a^2})} \\
 & \overline{(a^3b-ab^3-a^2b^2-a,\ \boldsymbol{-b^2})} \\
 & -\ \underline{(-a^2b^2-b,\ \boldsymbol{-b^2})} \\
 & \overline{(a^3b-ab^3-a+b,\ 0)}
\end{array}$$

That is,

$$f = af_1 - bf_2 + (a^3b - ab^3 - a + b,\ 0),$$

with respect to the given orderings.

At the end of section 4.2 of this chapter, we looked forward to obtaining *simple* bases for ideals in $\mathbb{F}[x_1,\ldots,x_k]$ (i.e. submodules of $\mathbb{F}[x_1,\ldots,x_k]$) that could easily help determine zero sets of such ideals. We are set to give a property of such bases, but before then, we consider some important notations.

Notation 4.3.18. Let M be a submodule of R^n different from $\{0\}$, and $>$ be a monomial order on R^n. The set of leading terms of all elements of M with respect to $>$ will be denoted by $\mathrm{LT}(M)$, i.e.

$$\mathrm{LT}(M) = \left\{cx^\alpha e_i \,:\, \exists\ f \in M \text{ with } \mathrm{LT}(f) = cx^\alpha e_i,\ c \in \mathbb{F}\right\},$$

so that $\langle \mathrm{LT}(M)\rangle$ will be the monomial submodule generated by elements in $\mathrm{LT}(M)$.

Definition 4.3.19. Let M be a submodule of R^n, and $>$ be a fixed monomial order on R^n. A finite subset $G = \{g_1,\ldots,g_s\} \subseteq M$ is called a **Gröbner basis** for M if

$$\langle \mathrm{LT}(M)\rangle = \langle \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_s)\rangle.$$

Proposition 4.3.20. *Let $G = \{g_1, \ldots, g_s\}$ be a Gröbner basis for a submodule $M \subseteq R^n$, and f be an arbitrary element in R^n. Then f belongs to M if and only if the remainder on division by G is zero.*

Proof. Suppose f is divided by the finite subset $G = \{g_1, \ldots, g_s\} \subseteq M$. Then by Theorem 4.3.15 (the division algorithm in R^n), f can be written as $f = a_1 g_1 + \ldots + a_s g_s + r$, where $a_i \in R$, $r \in R^n$, $\mathrm{LT}(a_i g_i) \geq \mathrm{LT}(f)$ for all i, $1 \leq i \leq s$, and either $r = 0$ or r is a $\mathbb{F}$-linear combination of monomials, none of which is divisible by any of $\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s)$. First, if $r = 0$, then $f = a_1 g_1 + \ldots + a_s g_s$ and so f belongs to $\langle G \rangle \subseteq M$, i.e. $f \in M$. Suppose on the other hand that f belongs to M. Then $\mathrm{LT}(f)$ belongs to $\langle \mathrm{LT}(M) \rangle$, by definition. Rewrite $f = a_1 g_1 + \cdots + a_s g_s + r$ as $r = f - (a_1 g_1 + \cdots + a_s g_s)$. If $r \neq 0$, then $\mathrm{LT}(r)$ belongs to $\langle \mathrm{LT}(M) \rangle$, since $f - (a_1 g_1 + \cdots + a_s g_s)$ belongs to M, M being a submodule. This further implies that $\mathrm{LT}(r)$ belongs to $\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$, since $\langle \mathrm{LT}(M) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$, $\{g_1, \ldots, g_s\}$ being a Gröbner basis for M. That is, $\mathrm{LT}(r)$ is divisible by some $\mathrm{LT}(g_i)$, $1 \leq i \leq s$. This contradicts the definition of a remainder, and so r has to be zero. □

Theorem 4.3.21. *Every submodule of R^n is finitely generated.*

Proof. Suppose M is an arbitrary submodule of R^n. From Notation 4.3.18, $\langle \mathrm{LT}(M) \rangle$ is a monomial submodule of R^n, and so by Proposition 4.3.13 (a), there exists a finite collection $\{X_1, \ldots, X_s\}$ of monomials in R^n that generates $\langle \mathrm{LT}(M) \rangle$, i.e $\langle \mathrm{LT}(M) \rangle = \langle X_1, \ldots, X_s \rangle$. Now, for $1 \leq i \leq s$, let f_i be an element in M with $\mathrm{LT}(f_i) = X_i$, that is, $\langle \mathrm{LT}(M) \rangle = \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle$. Then by Definition 4.3.19, the finite subset $\{f_1, \ldots, f_s\} \subseteq M$ becomes a Gröbner basis for M. Consequently, $\langle f_1, \ldots, f_s \rangle \subseteq M$. It will now be shown that $M \subseteq \langle f_1, \ldots, f_s \rangle$. To this end, let f be an arbitrary element in M. Then from the proof of Proposition 4.3.20, f belongs to $\langle f_1, \ldots, f_s \rangle$, since $\{f_1, \ldots, f_s\}$ is a Gröbner basis for M. Therefore, $M = \langle f_1, \ldots, f_s \rangle$ for some finite subset $\{f_1, \ldots, f_s\} \subseteq M$, i.e. M is finitely generated. Since M is chosen arbitrarily, we conclude that every submodule of R^n is finitely generated. □

It is important to note that Gröbner bases for a submodule M of R^n need not to be R-linearly independent, though they generate M as an R-module in its own right.

Theorem 4.3.22 (Ascending Chain Condition)**.** *Every infinite ascending chains $M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$ of submodules of R^n stabilizes. That is, there exists N_0 such that $M_N = M_{N_0}$ for all $N \geq N_0$.*

Proof. Let $M = \bigcup_{i=1}^{\infty} M_i$, where each M_i is a submodule of R^n. It will be shown that M is also a submodule of R^n. First, the zero element in R^n belongs to M, since 0 belongs to each M_i, $i \geq 1$. Now, let f, g be any elements in M. Then f and g belong to M_i and M_j, respectively for some $i, j \geq 1$. Assuming $i \leq j$, then M_i is contained in M_j by the ascending chain $M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$. Consequently, f belongs to M_j, and thus, rf belongs to M_j for all $r \in R$, since M_j is a submodule of R^n. Furthermore, $rf - g$ belongs to M_j, since both rf and g are in M_j, and M_j is a submodule of R^n. Therefore, $rf - g$ belongs to M, since M_j is contained in M. So M is also a submodule of R^n, and so by Theorem 4.3.21, M is generated by a finite subset, say $\{f_1, \ldots, f_s\} \subseteq R^n$, i.e. $M = \langle f_1, \ldots, f_s \rangle$, for some $s \geq 1$. For each j, $1 \leq j \leq s$, f_j belongs to M_{i_j} for some $i_j \geq 1$. Setting $N_0 := \max_{1 \leq j \leq s}\{i_j\}$, then f_j belongs to M_{N_0} for all j, $1 \leq j \leq s$. Therefore,

$$\bigcup_{i=1}^{\infty} M_i = M = \langle f_1, f_2, \ldots, f_s \rangle \subseteq M_{N_0} \subseteq M_{N_0+1} \subseteq \ldots \subseteq \bigcup_{i=1}^{\infty} M_i,$$

i.e.

$$M = \bigcup_{i=1}^{\infty} M_i \subseteq M_{N_0} \subseteq M_{N_0+1} \subseteq \ldots \subseteq \bigcup_{i=1}^{\infty} M_i = M,$$

implying $M_N = M_{N_0}$ for all $N \geq N_0$, as required. □

Finally in this section, an algorithm for computing Gröbner bases of submodules of R^n, which is just extension of the Buchberger's Algorithm (Theorem 2 in Section 7, Chapter 2 of [7]), will be considered.

Definition 4.3.23. Let a monomial order on R^n be fixed, and let f, g be elements in R^n. The **S-vector** of f and g, denoted $S(f, g)$, is an element of R^n which equals the combination

$$S(f, g) = \frac{\operatorname{lcm}\big(\mathrm{LM}(f), \mathrm{LM}(g)\big)}{\mathrm{LT}(f)} \cdot f - \frac{\operatorname{lcm}\big(\mathrm{LM}(f), \mathrm{LM}(g)\big)}{\mathrm{LT}(g)} \cdot g.$$

Example 4.3.24. Let $f = (ab^2 + 1, a)$ and $g = (a^2b + 1, b)$ be elements in $\mathbb{Q}[a, b]^2$. Assume $e_1 > e_2$, and let the lexicographic ordering, **lex** on $\mathbb{Q}[a, b]$, with $b \prec a$, be extended to a **POT**

Input: $F = \{f_1, \ldots, f_s\} \subseteq R^n$, *an order* $>$

Output: *A Gröbner basis* G *for* $M = \langle F \rangle$, *with respect to* $>$

Initialization: $G \leftarrow F$

REPEAT

$G' := G$

FOR each pair $\{f, g\}$, $f \neq g$ *in* G' *DO*

$S \leftarrow \overline{S(f,g)}^{G'}$

IF $S \neq 0$ *THEN* $G \leftarrow G \cup \{S\}$

UNTIL $G = G'$.

Algorithm 4.3: Buchberger's algorithm for submodules in R^n

ordering on $\mathbb{Q}[a,b]^2$. Then we obtain the following: $f = ab^2e_1 + e_1 + ae_2$ and $g = a^2be_1 + e_1 + be_2$ imply $\mathrm{LT}(f) = ab^2e_1$ and $\mathrm{LT}(g) = a^2be_1$, so that

$$\begin{aligned} S(f,g) &= \frac{\mathrm{lcm}\big(\mathrm{LM}(f), \mathrm{LM}(g)\big)}{\mathrm{LT}(f)} \cdot f - \frac{\mathrm{lcm}\big(\mathrm{LM}(f), \mathrm{LM}(g)\big)}{\mathrm{LT}(g)} \cdot g \\ &= \frac{a^2b^2}{ab^2} \cdot (ab^2 + 1, a) - \frac{a^2b^2}{a^2b} \cdot (a^2b + 1, b) \\ &= a \cdot (ab^2 + 1, a) - b \cdot (a^2b + 1, b) = (a - b, a^2 - b^2). \end{aligned}$$

Theorem 4.3.25 (Buchberger's Criterion for Submodules)**.** *A set* $G = \{g_1, \ldots, g_s\} \subseteq R^n$ *is a Gröbner basis for the submodule it generates if and only if the remainder on division by* G *of* $S(g_i, g_j)$ *is zero, for all* $i \neq j$.

Proof. The proof is the same as in the case of $n = 1$ (Theorem 6 in Section 6, Chapter 2 of [7]). □

For example, the set $\{f, g\} \subseteq \mathbb{Q}[a,b]^2$, where f and g are as in Example 4.3.24, is not a Gröbner basis for the submodule it generates in $\mathbb{Q}[a,b]^2$, with respect to the given ordering. The reason is that the remainder of $S(f,g)$ on division by $\{f, g\} \subseteq \mathbb{Q}[a,b]^2$ does not equal 0.

Theorem 4.3.26 (Buchberger's Algorithm for Submodules)**.** *Let* $F = \{f_1, \ldots, f_s\}$ *where* $f_i \in R^n$, *and fix a monomial order on* R^n. *Algorithm 4.3 computes a Gröbner basis* G *for* $M = \langle F \rangle \subseteq R^n$, *where* $\overline{S(f,g)}^{G'}$ *denotes the remainder on division of* $S(f,g)$ *by* G'.

Proof. The proof is also the same as in the case of $n = 1$ (Theorem 2 in Section 7, Chapter 2 of [7]). Part (b) of Proposition 4.3.13 ensures termination of the algorithm. □

Example 4.3.27. Revisiting Example 4.3.24, let $G = \{f, g\}$, where $f = (ab^2 + 1, a)$ and $g = (a^2b + 1, b)$ are elements in $\mathbb{Q}[a, b]^2$. Assume $e_1 > e_2$, and let the lexicographic ordering, **lex** on $\mathbb{Q}[a, b]$, with $b \prec a$, be extended to a **POT** ordering on $\mathbb{Q}[a, b]^2$. Using Algorithm 4.3, we first set $G' := G$. Taking the pair $\{f, g\}$ in G', $S(f, g)$ equals $(a-b, a^2-b^2)$, from Example 4.3.24. The remainder of $S(f, g)$ on division by G' is not 0, and in fact equals $S(f, g)$ itself, reason being that the leading term of $S(f, g)$, which is ae_1, is not divisible by any of ab^2e_1 and a^2be_1, which are the leading terms of f and g respectively. In other words, $\overline{S(f,g)}^{G'} = S(f, g)$, and so $S(f, g)$ is appended to G, i.e. $G = \{f, g, S(f, g)\}$. Next, we set $G' := G$, and consider the two pairs $\{f, h_1\}$ and $\{g, h_1\}$ in G', where $h_1 = S(f, g)$. Since $S(f, h_1) = (b^3 + 1, -a^2b^2 + a + b^4)$ and $S(g, h_1) = (ab^2 + 1, -a^3b + ab^3 + b) = f + (0, -a^3b + ab^3 - a + b)$, we obtain $\overline{S(f,h_1)}^{G'} = S(f, h_1)$ (since $\mathrm{LT}\,(S(f, h_1)) = b^3e_1$ is not divisible by any of the leading terms of f, g and h) and $\overline{S(g,h_1)}^{G'} = (0, -a^3b+ab^3-a+b)$. Therefore, both $S(f, h_1)$ and $(0, -a^3b+ab^3-a+b)$ are appended to G, i.e. $G = \{f, g, h_1, h_2, h_3\}$, where $h_2 = S(f, h_1)$ and $h_3 = (0, -a^3b + ab^3 - a + b)$. We set again $G' := G$. Considering the pairs $\{f, h_2\}$, $\{f, h_3\}$, $\{g, h_2\}$, $\{g, h_3\}$, $\{h_1, h_2\}$, $\{h_1, h_3\}$ and $\{h_2, h_3\}$ in G', we obtain the following:

$S(f, h_2) = (-a + b, a^3b^2 - a^2 - ab^4 + ab) = -h_1 - bh_3 \implies \overline{S(f,h_2)}^{G'} = 0.$

$S(f, h_3) = 0,$ since both leading terms of f and h_3 contain different e_i, $i = 1, 2.$

$S(g, h_2) = (2a^2b^3 + a^2 + b^2, -a^4b^2 + a^3 + a^2b^4 + b^3) = 2abf + (a - b)h_1 + abh_3$
$\implies \overline{S(g,h_2)}^{G'} = 0.$

$S(g, h_3) = 0,$ since both leading terms of g and h_3 contain different e_i, $i = 1, 2.$

$S(h_1, h_2) = (-a - b^4, a^3b^2 + a^2b^3 - a^2 - ab^4 - b^5) = -h_1 - bh_2 - bh_3 \implies \overline{S(h_1,h_2)}^{G'} = 0.$

$S(h_1, h_3) = 0,$ since both leading terms of h_1 and h_3 contain different e_i, $i = 1, 2.$

$S(h_2, h_3) = 0,$ since both leading terms of h_2 and h_3 contain different e_i, $i = 1, 2.$

Since the vectors $S(f, h_3)$, $S(g, h_3)$ and $S(h_2, h_3)$ are all 0, the remainder on division of these zero vectors by G' is just 0. Hence, the finite subset $G = \{f, g, h_1, h_2, h_3\}$ is a Gröbner basis for the submodule of $\mathbb{Q}[a, b]^2$ generated by $\{f, g\}$, with respect to the given monomial ordering on $\mathbb{Q}[a, b]^2$.

Definition 4.3.28. Let M be a submodule of R^n, and $>$ be a fixed monomial order on R^n. A Gröbner basis for M is called a **minimal Gröbner basis** for M if:

(i) $\mathrm{LC}(g) = 1$ for all $g \in G$, and

(ii) $\mathrm{LT}(g) \notin \langle \mathrm{LT}(G - \{g\}) \rangle$, for all $g \in G$.

Example 4.3.29. From Example 4.3.27, since $\mathrm{LT}(f) = ab^2e_1 = b^2 \cdot \mathrm{LT}(h_1)$ and $\mathrm{LT}(g) = a^2be_1 = ab \cdot \mathrm{LT}(h_1)$, both f and g can be removed from the set of basis $G = \{f, g, h_1, h_2, h_3\}$, so that the finite subset

$$\{h_1, h_2, -h_3\} = \{(a-b, a^2-b^2), (b^3+1, -a^2b^2+a+b^4), (0, a^3b-ab^3+a-b)\} \subseteq \mathbb{Q}[a,b]^2$$

becomes a minimal Gröbner basis for the submodule of $\mathbb{Q}[a,b]^2$ generated by $\{f, g\}$, with respect to the given monomial ordering on $\mathbb{Q}[a,b]^2$.

Definition 4.3.30. Let M be a submodule of R^n, and $>$ be a fixed monomial order on R^n. A Gröbner basis for M is called a **reduced Gröbner basis** for M if:

(i) $\mathrm{LC}(g) = 1$ for all $g \in G$, and

(ii) no monomial of g lies in $\langle \mathrm{LT}(G - \{g\}) \rangle$, for all $g \in G$.

Example 4.3.31. From Example 4.3.29, we obtain a minimal Gröbner basis $G = \{h_1, h_2, -h_3\}$ for the submodule of $\mathbb{Q}[a,b]^2$ generated by $\{f, g\}$, with respect to the given monomial ordering on $\mathbb{Q}[a,b]^2$, where f and g are as in Example 4.3.27. In fact, this minimal basis is a reduced Gröbner basis, reason being that no monomial of g is divisible by any monomial in $\langle \mathrm{LT}(G - \{g\}) \rangle$, for all $g \in G = \{h_1, h_2, -h_3\}$.

Example 4.3.32. In Section 4.2 of this thesis, a partial Smith form of a matrix was obtained (Example 4.2.2). The set of nonzero entries in the lower right block matrix B of the partial Smith form obtained is

$$\begin{aligned} S \;=\; \big\{ & x_1^2 - x_3,\; x_2^2 - x_1x_2 + x_3,\; -x_2^2 + x_4,\; x_1x_2 - x_1^2 - x_4,\; -x_1^2x_3 - x_1x_3 + x_2x_3, \\ & -x_1x_2x_3 - x_2x_3 + x_1x_4,\; -x_1x_3^2 - x_1x_4 + x_2x_4,\; -x_1x_3x_4 - x_2x_4 \big\}, \end{aligned}$$

a subset of $\mathbb{F}[x_1, x_2, x_3, x_4]$. With the help of a computer algebra system, the reduced Gröbner basis for the ideal generated by set S with respect to lexicographic (lex) ordering with $x_1 < x_2 < x_3 < x_4$ is:

$$G = \big\{ x_1^3(x_1^2 + x_1 + 1),\; x_1^2(x_2 - x_1^2 - x_1),\; x_2^2 - x_1x_2 + x_1^2,\; x_3 + x_2^2 - x_1x_2,\; x_4 - x_1x_2 + x_1^2 \big\}.$$

The brief study of Gröbner basis for free modules $\mathbb{F}[x_1, \ldots, x_k]^n$, $n \geq 1$ was considered in the first place, primarily because we want to compute easily the zero set of a certain ideal – the ideal generated by entries in lower right block matrix B of the partial Smith form obtained in Example 4.2.2.

If we denote the set of all common zeros of polynomials in an arbitrary ideal $I = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_k]$ by $\mathbb{V}(I)$, i.e.

$$\mathbb{V}(I) = \big\{(a_1, \ldots, a_k) \in \mathbb{F}^k \,:\, f(a_1, \ldots, a_k) = 0 \text{ for all } f \in I\big\},$$

then it can be shown that $\mathbb{V}(I) = \mathbb{V}(f_1, \ldots, f_s)$. In fact, suppose first $(a_1, \ldots, a_k)$ belongs to $\mathbb{V}(I)$. Then by definition, $f(a_1, \ldots, a_k) = 0$ for all $f \in I$. In particular, $f_i(a_1, \ldots, a_k) = 0$ for all $i = 1, \ldots, s$, since each f_i $(1 \leq i \leq s)$ belongs to I. Hence, $\mathbb{V}(I) \subseteq \mathbb{V}(f_1, \ldots, f_s)$. Suppose on the other hand, $(a_1, \ldots, a_k)$ belongs to $\mathbb{V}(f_1, \ldots, f_s)$. Then, by definition, $f_i(a_1, \ldots, a_k) = 0$ for all $i = 1, \ldots, s$. If f is an arbitrary element in I, then $f = r_1 f_1 + \cdots + r_s f_s$, for some $r_1, \ldots, r_s$ in $\mathbb{F}[x_1, \ldots, x_k]$. Consequently, $f(a_1, \ldots, a_k) = 0$ since $r_i(a_1, \ldots, a_k) f_i(a_1, \ldots, a_k) = r_i(a_1, \ldots, a_k) \cdot 0 = 0$ for each i, $1 \leq i \leq s$. Hence, $(a_1, \ldots, a_k)$ belongs to $\mathbb{V}(I)$, since f is arbitrarily chosen. Therefore, $\mathbb{V}(f_1, \ldots, f_s) \subseteq \mathbb{V}(I)$.

As a result of the above paragraph, computing common zeros for the entries in set S in Example 4.3.32, is equivalent to computing the zero set for an ideal generated by the set S. Therefore, the set of all common zeros of the entries in set S equals $\mathbb{V}(G)$, where

$$G = \big\{x_1^3(x_1^2 + x_1 + 1),\, x_1^2(x_2 - x_1^2 - x_1),\, x_2^2 - x_1x_2 + x_1^2,\, x_3 + x_2^2 - x_1x_2,\, x_4 - x_1x_2 + x_1^2\big\},$$

is the reduced Gröbner basis for the ideal generated by set S with respect to lexicographic (lex) ordering with $x_1 < x_2 < x_3 < x_4$. The set $\mathbb{V}(G)$ is computed as follows:

$$x_1^3(x_1^2 + x_1 + 1) = 0 \tag{4.2}$$

$$x_1^2(x_2 - x_1^2 - x_1) = 0 \tag{4.3}$$

$$x_2^2 - x_1x_2 + x_1^2 = 0 \tag{4.4}$$

$$x_3 + x_2^2 - x_1x_2 = 0 \tag{4.5}$$

$$x_4 - x_1x_2 + x_1^2 = 0 \tag{4.6}$$

From equation (4.2), either $x_1 = 0$ or $x_1 = \omega$, where $\omega = -\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$. Substituting 0 for x_1 in equation (4.3), we obtain $x_2 = 0$. However, substituting ω for x_1 in equation (4.3), we obtain

$x_2 - \omega^2 - \omega = 0$, implying $x_2 = \omega^2 + \omega = -1$, since ω satisfies $\omega^2 + \omega + 1 = 0$. Substituting $(0, 0)$ for (x_1, x_2) in equation (4.5), we obtain $x_3 = 0$. But substituting $(\omega, -1)$ for (x_1, x_2) in equation (4.5), we obtain $x_3 + (-1)(-1 - \omega) = 0$, which implies $x_3 = -\omega - 1 = \omega^2$. If we substitute $(0, 0, 0)$ for (x_1, x_2, x_3) in equation (4.6), we will obtain $x_4 = 0$. But substituting $(\omega, -1, \omega^2)$ for (x_1, x_2, x_3) in equation (4.6), we will obtain $x_4 - \omega(-1 - \omega) = 0$, implying $x_4 = -\omega - \omega^2 = 1$. Therefore, we obtain the set of three points

$$V(G) = \big\{(0, 0, 0, 0),\, (\omega, -1, \omega^2, 1)\big\},$$

where $\omega = -\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$, as the set of common roots of all polynomials in S.

Now, revisiting fully Example 4.2.2, where

$$A = \begin{bmatrix} 1 & x_1 & x_2 & x_3 & x_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & x_1 & 0 & 0 & x_2 & 0 & x_3 & x_4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & x_1 & 0 & 0 & x_2 & 0 & 0 & x_3 & 0 & x_4 & 0 & 0 \\ 0 & 0 & 1 & 0 & x_1 & 0 & 0 & x_2 & 0 & 0 & x_3 & 0 & x_4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & x_1 & 0 & x_2 & 0 & 0 & x_3 & 0 & x_4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & x_1 & x_2 & x_3 & x_4 \end{bmatrix}$$

is a 6×14 matrix over $\mathbb{F}[x_1, x_2, x_3, x_4]$, we obtain a partial Smith form of matrix A to be matrix

$$P = \left[\begin{array}{c|c} I_5 & O_{5,9} \\ \hline O_{1,5} & B_{1,9} \end{array}\right],$$

where $B_{1,9}$ is the 1×9 matrix

$$B^t = \begin{bmatrix} x_1^2 - x_3 \\ 0 \\ x_2^2 - x_1x_2 + x_3 \\ -x_2^2 + x_4 \\ x_1x_2 - x_1^2 - x_4 \\ -x_1^2x_3 + x_2x_3 - x_1x_3 \\ -x_1x_2x_3 - x_2x_3 + x_1x_4 \\ -x_1x_3^2 - x_1x_4 + x_2x_4 \\ -x_1x_3x_4 - x_2x_4 \end{bmatrix}.$$

Using the set $\mathbb{V}(G)$ obtained above, matrix B will only be a zero matrix provided (x_1, x_2, x_3, x_4) belongs to $\mathbb{V}(G)$. To be more precise, if $\mathbb{F} = \mathbb{Q}$ or $\mathbb{R}$, then matrix B will only equal zero

matrix provided $(x_1, x_2, x_3, x_4) = (0, 0, 0, 0)$. But if $\mathbb{F} = \mathbb{C}$, then matrix B will only be a zero matrix provided (x_1, x_2, x_3, x_4) belongs to $\mathbb{V}(G)$.

Finally in this chapter, Examples 4.3.24, 4.3.27, 4.3.29 and 4.3.31 will be translated to matrix operations. This will naturally lead to an algorithm (matrix form) for computing Gröbner basis for submodules of free modules over $\mathbb{F}[x_1, \ldots, x_k]$. The algorithm is originally stated in Section 8.4.3 of [3] (Algorithm 8.4.3.2).

Example 4.3.33. Let

$$A = \begin{bmatrix} ab^2{+}1 & a \\ a^2b{+}1 & b \end{bmatrix}$$

be a 2×2 matrix over $\mathbb{Q}[a, b]^2$. Assume $e_1 > e_2$, and let the lexicographic ordering, **lex** on $\mathbb{Q}[a, b]$, with $b \prec a$, be extended to a **POT** ordering on $\mathbb{Q}[a, b]^2$. The rows of matrix A are the two vectors whose Gröbner basis are computed in Example 4.3.27. Following strictly Example 4.3.27, there is a need to first compute S-vector of the two row vectors of A, and then determine its remainder on division by the row vectors of A. In order to translate this particular computation to matrix operation, it is necessary to first create a new zero row at the bottom of matrix A, which gives matrix A_1 below. Next, according to Example 4.3.24, we multiply row 1 of matrix A_1 by a and then add the result to row 3. This gives matrix A_2 below. And still according to Example 4.3.24, multiplying row 2 of matrix A_2 by $-b$ and then adding the result to row 3, yield matrix A_3 below.

$$A_1 = \begin{bmatrix} ab^2{+}1 & a \\ a^2b{+}1 & b \\ 0 & 0 \end{bmatrix} \longrightarrow A_2 = \begin{bmatrix} ab^2{+}1 & a \\ a^2b{+}1 & b \\ a(ab^2{+}1) & a^2 \end{bmatrix} \longrightarrow A_3 = \begin{bmatrix} ab^2{+}1 & a \\ a^2b{+}1 & b \\ a{-}b & a^2{-}b^2 \end{bmatrix}.$$

Next, according to Example 4.3.27, there is a need to compute S-vectors for rows 1 and 3, and rows 2 and 3 of matrix A_3, and thereafter determine their remainders on division by rows of matrix A_3. First, for S-vectors of rows 1 and 3 of matrix A_3, a new zero row is created at the bottom of matrix A_3, which gives matrix A_4 below. Multiplying row 1 of matrix A_4 by $\frac{\text{lcm}(ab^2,a)}{ab^2} = 1$ and then adding the result to row 4, yield matrix A_5 below. Now, multiplying row 3 of matrix A_5 by $-\frac{\text{lcm}(ab^2,a)}{a} = -b^2$ and then adding the result to row 4, give matrix A_6

below.

$$A_4 = \begin{bmatrix} ab^2+1 & a \\ a^2b+1 & b \\ a-b & a^2-b^2 \\ 0 & 0 \end{bmatrix} \longrightarrow A_5 = \begin{bmatrix} ab^2+1 & a \\ a^2b+1 & b \\ a-b & a^2-b^2 \\ ab^2+1 & a \end{bmatrix} \longrightarrow A_6 = \begin{bmatrix} ab^2+1 & a \\ a^2b+1 & b \\ a-b & a^2-b^2 \\ b^3+1 & -a^2b^2+a+b^4 \end{bmatrix}.$$

For S-vectors of rows 2 and 3 of matrix A_3 (which are just rows 2 and 3 of matrix A_6), a new zero row is created at the bottom of matrix A_6, which gives matrix A_7 below. Multiplying row 2 of matrix A_7 by $\frac{\text{lcm}(a^2b,a)}{a^2b} = 1$ and then adding the result to row 5, yield matrix A_8 below. Multiplying row 3 of matrix A_8 by $-\frac{\text{lcm}(a^2b,a)}{a} = -ab$ and then adding the result to row 5, give matrix A_9 below.

$$A_7 = \begin{bmatrix} ab^2+1 & a \\ a^2b+1 & b \\ a-b & a^2-b^2 \\ b^3+1 & -a^2b^2+a+b^4 \\ 0 & 0 \end{bmatrix} \longrightarrow A_8 = \begin{bmatrix} ab^2+1 & a \\ a^2b+1 & b \\ a-b & a^2-b^2 \\ b^3+1 & -a^2b^2+a+b^4 \\ a^2b+1 & b \end{bmatrix} \longrightarrow A_9 = \begin{bmatrix} ab^2+1 & a \\ a^2b+1 & b \\ a-b & a^2-b^2 \\ b^3+1 & -a^2b^2+a+b^4 \\ ab^2+1 & -a^3b+ab^3+b \end{bmatrix}.$$

Now, unlike row 3 of matrix A_3 relative to rows 1 and 2 of same matrix, and row 4 of matrix A_6 relative to rows 1, 2 and 3 of same matrix, row 5 of matrix A_9 needs to be reduced further by replacing it with its remainder on division by rows 1, 2 and 3 of matrix A_9. In fact, multiplying row 1 of matrix A_9 by -1 and then adding the result to row 5, we obtain matrix A_{10} below.

$$A_{10} = \begin{bmatrix} ab^2+1 & a \\ a^2b+1 & b \\ a-b & a^2-b^2 \\ b^3+1 & -a^2b^2+a+b^4 \\ 0 & -a^3b+ab^3-a+b \end{bmatrix}.$$

From Example 4.3.27, the S-vectors for rows 1 and 4, rows 1 and 5, rows 2 and 4, rows 2 and 5, and rows 3 and 4, rows 3 and 5, and rows 4 and 5, all became zero after division by row vectors in rows 1, 2, 3, 4 and 5 of matrix A_{10}. Hence, the submodule of $\mathbb{Q}[a,b]^2$ generated by the five rows of matrix A_{10} is a Gröbner basis (though not a reduced Gröbner basis according to Definition 4.3.30) for the submodule of $\mathbb{Q}[a,b]^2$ generated by the two rows of the original matrix A, with respect to the given monomial ordering on $\mathbb{Q}[a,b]^2$. We now press forward to obtain a reduced Gröbner basis. Multiplying row 3 of matrix A_{10} by $-b^2$, and then adding

the result to row 1, we obtain below matrix A_{11}. Multiplying row 4 of matrix A_{11} by -1, and then adding the result to row 1, we obtain below matrix A_{12}.

$$A_{11} = \begin{bmatrix} b^3{+}1 & -a^2b^2{+}a{+}b^4 \\ a^2b{+}1 & b \\ a{-}b & a^2{-}b^2 \\ b^3{+}1 & -a^2b^2{+}a{+}b^4 \\ 0 & -a^3b{+}ab^3{-}a{+}b \end{bmatrix} \longrightarrow A_{12} = \begin{bmatrix} 0 & 0 \\ a^2b{+}1 & b \\ a{-}b & a^2{-}b^2 \\ b^3{+}1 & -a^2b^2{+}a{+}b^4 \\ 0 & -a^3b{+}ab^3{-}a{+}b \end{bmatrix}.$$

Next, multiplying row 3 of matrix A_{12} by $-ab - b^2$, and then adding the result to row 2, we obtain below matrix A_{13}. Multiplying row 4 of matrix A_{13} by -1, and then adding the result to row 2, we obtain below matrix A_{14}.

$$A_{13} = \begin{bmatrix} 0 & 0 \\ b^3{+}1 & -a^3b{-}a^2b^2{+}ab^3{+}b^4{+}b \\ a{-}b & a^2{-}b^2 \\ b^3{+}1 & -a^2b^2{+}a{+}b^4 \\ 0 & -a^3b{+}ab^3{-}a{+}b \end{bmatrix} \longrightarrow A_{14} = \begin{bmatrix} 0 & 0 \\ 0 & -a^3b{+}ab^3{-}a{+}b \\ a{-}b & a^2{-}b^2 \\ b^3{+}1 & -a^2b^2{+}a{+}b^4 \\ 0 & -a^3b{+}ab^3{-}a{+}b \end{bmatrix}.$$

Multiplying row 5 of matrix A_{14} by -1, and then adding the result to row 2, we obtain below matrix A_{15}. Next, multiplying row 5 of matrix A_{15} by -1, we finally obtain below matrix A_{16}, which is a reduced Gröbner basis for the submodule of $\mathbb{Q}[a,b]^2$ generated by the 2 rows of the original matrix A (the first 2 rows of matrix A_{15} have been deleted, since they are now zero rows).

$$A_{15} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ a{-}b & a^2{-}b^2 \\ b^3{+}1 & -a^2b^2{+}a{+}b^4 \\ 0 & -a^3b{+}ab^3{-}a{+}b \end{bmatrix} \longrightarrow A_{16} = \begin{bmatrix} a{-}b & a^2{-}b^2 \\ b^3{+}1 & -a^2b^2{+}a{+}b^4 \\ 0 & a^3b{-}ab^3{+}a{-}b \end{bmatrix}.$$

This completes the example.

The steps performed in the example above coincide with the steps in Algorithm 8.4.3.2 of [3]. In fact, if A is an arbitrary $m \times n$ matrix over the ring of polynomials $\mathbb{F}[x_1, \ldots, x_k]$, assume $e_1 > e_2 > \cdots > e_n$ as an ordering on the column of matrix A, and if any given monomial ordering on $\mathbb{F}[x_1, \ldots, x_k]^n$ is extended to a **POT** ordering on $\mathbb{F}[x_1, \ldots, x_k]^n$, then

Algorithm 8.4.3.2 in Section 8.4.3 of [3] coincides with Algorithm 4.3 (Buchberger's algorithm for submodules in $\mathbb{F}[x_1, \ldots, x_k]^n$), except that while the former always gives a reduced Gröbner basis for submodules, the latter sometimes does not. The former algorithm (Algorithm 8.4.3.2 in Section 8.4.3 of [3]) is reproduced here as Algorithm 4.4, and an example is given to illustrate the algorithm. With this, we conclude this thesis.

Example 4.3.34. Let

$$A = \begin{bmatrix} b & 0 & 0 & 0 \\ b^2 & ab & 1 & a+1 \\ ab+b^2 & 1 & 0 & b \\ ab & b & 0 & b^2 \end{bmatrix}$$

be a 4×4 matrix over $\mathbb{Q}[a, b]$, with lexicographic monomial ordering $b \prec a$. The first pivot is $(1, 1)$. The ideal generated by entries in position $(i, 1)$, $1 \leq i \leq 4$ is the principal ideal $\langle b \rangle$. Therefore, adding $-b$ times row 1 to row 2, adding $-(a+b)$ times row 1 to row 3, and adding $-a$ times row 1 to row 4, we obtain:

$$\begin{bmatrix} b & 0 & 0 & 0 \\ 0 & ab & 1 & a+1 \\ ab+b^2 & 1 & 0 & b \\ ab & b & 0 & b^2 \end{bmatrix} \longrightarrow \begin{bmatrix} b & 0 & 0 & 0 \\ 0 & ab & 1 & a+1 \\ 0 & 1 & 0 & b \\ ab & b & 0 & b^2 \end{bmatrix} \longrightarrow \begin{bmatrix} b & 0 & 0 & 0 \\ 0 & ab & 1 & a+1 \\ 0 & 1 & 0 & b \\ 0 & b & 0 & b^2 \end{bmatrix}.$$

The next pivot is $(2, 2)$. The smallest nonzero entry among the entries in position $(i, 2)$, $2 \leq i \leq 4$ is 1, and it is in row 3. Thus, rows 2 and 3 are swapped, to obtain:

$$\begin{bmatrix} b & 0 & 0 & 0 \\ 0 & 1 & 0 & b \\ 0 & ab & 1 & a+1 \\ 0 & b & 0 & b^2 \end{bmatrix}.$$

The ideal generated by entries in position $(i, 2)$, $2 \leq i \leq 4$ is the principal ideal $\langle 1 \rangle$. Therefore, adding $-ab$ times row 2 to row 3, and adding $-b$ times row 2 to row 4, we obtain:

$$\begin{bmatrix} b & 0 & 0 & 0 \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & -ab^2+a+1 \\ 0 & b & 0 & b^2 \end{bmatrix} \longrightarrow \begin{bmatrix} b & 0 & 0 & 0 \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & -ab^2+a+1 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Input: An $m \times n$ matrix A with entries in $\mathbb{F}[x_1, \ldots, x_k]$.

Output: The Gröbner basis for row(A), with respect to the given (implicit) order of the columns and some given monomial order.

Initialization: Set $i \leftarrow 1$, $j \leftarrow 1$.

- While $i \leq m$ and $j \leq n$ do:
  1. If all entries at and below pivot (i, j) are 0, then set $j \leftarrow j + 1$.
  2. Otherwise:
     (a) Repeat until stabilization: Use row operations to swap the smallest nonzero entry into the pivot and reduce the other entries modulo the pivot.
     (b) Sort the entries at and below the pivot in increasing order, with 0 being the greatest.
     (c) For $k = 1, \ldots, m-i$, repeat the two previous steps ((a) and (b)) for the entries at and below position $(i+k, j)$ to self-reduce the column.
     (d) For every pair of indices k, k' such that $i \leq k \neq k' \leq m$ and the entries in positions (i, k) and (i, k') produce an S-polynomial with a nonzero reduced form modulo the entries in rows i through m, do the following:
        i. Set $m \leftarrow m+1$; add a new zero row at the bottom.
        ii. Use row operations to construct the S-polynomial in position $(m+1, j)$, and compute its nonzero reduced form modulo the entries in rows i through m.
     (e) Repeat steps (a)–(d) until the entries at and below the pivot form a reduced Gröbner basis for the ideal they generate.
     (f) Delete any zero rows and modify m accordingly.
     (g) Use the Gröbner basis at and below the pivot to reduce the entries above the pivot to their normal forms.
     (h) Set $i \leftarrow i+1$, $j \leftarrow j+1$.

Algorithm 4.4: Submodule Gröbner basis algorithm (matrix form)

This completes the execution of the algorithm, and from the output we conclude that the submodule rowmod(A) generated by the rows of the original matrix A is free of rank 3, the reason being that in each column of the last matrix, the leading entry has only a single element.

4.4 Application of Gröbner bases for submodules of R^n, $n \geq 1$, $R = \mathbb{F}[x_1, \ldots, x_k]$

According to Cox et al. [7] (Page 93, Section 7, Chapter 2), one of the consequences of the uniqueness of reduced Gröbner basis is the **ideal equality algorithm.** This algorithm helps to tell if two ideals with different (finite) generators, say $\{f_1, \ldots, f_s\}$ and $\{g_1, \ldots, g_t\}$, are the same or not. Basically, a monomial order is fixed, and a reduced Gröbner basis is computed for the ideals $\langle f_1, \ldots, f_s \rangle$ and $\langle g_1, \ldots, g_t \rangle$; these ideals are the same if and only if they have the same reduced Gröbner bases.

The same proof for Proposition 6 in [7] (Page 92, Section 7, Chapter 2) can be used to show that for a fixed monomial order on R^n, every submodule $M \neq \{0\}$ of R^n has a unique reduced Gröbner basis (Definition 4.3.30). Consequently, we have an analogue for the ideal equality algorithm, which we call **row module equality algorithm**. Recall from Definition 3.3.30, the row module of an $m \times n$ matrix A over the polynomial ring $R = \mathbb{F}[x_1, \ldots, x_k]$, denoted rowmod($A$), is a submodule of R^n generated by the m rows of A.

Therefore, we formulate the row module equality algorithm as follows: Given a fixed monomial order on R^n and given two $m \times n$ matrices A and B over $R = \mathbb{F}[x_1, \ldots, x_k]$, then the row module of A equals the row module of B if and only if A and B have the same reduced Gröbner basis. In other words, for a fixed monomial order on R^n, the row modules of matrices A and B will be equal if and only if both A and B have the same canonical form, computed with the help of either Algorithm 4.3 or Algorithm 4.4. For the former algorithm, efforts need to still be made, if necessary, in order to obtain a *reduced* Gröbner basis, according to Definition 4.3.30.

References

[1] William Adkins and Steven Weintraub. *Algebra: an approach via module theory. Graduate Texts in Mathematics*, volume 136. Springer Science & Business Media, 2012.

[2] Bernhard. Banaschewski. A new proof that "Krull implies Zorn. *Mathematical Logic Quarterly*, 40(4):478–480, 1994.

[3] Murray R. Bremner and Vladimir Dotsenko. *Algebraic operads: an algorithmic companion*. CRC Press, 2016.

[4] Murray R. Bremner and Luiz A. Peresi. An application of lattice basis reduction to polynomial identities for algebraic structures. *Linear Algebra and its Applications*, 430(2):642–659, 2009.

[5] Paul J. Campbell. The origin of Zorn's lemma. *Historia Mathematica*, 5(1):77–89, 1978.

[6] Richard G. Cooke. *Infinite matrices and sequence spaces*. Courier Corporation, 2014.

[7] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms. Undergraduate Texts in Mathematics*, volume 3. Springer, 1992.

[8] David A. Cox, John Little, and Donal O'Shea. *Using algebraic geometry. Graduate Texts in Mathematics*, volume 185. Springer Science & Business Media, 2006.

[9] Marcel Erné. A primrose path from Krull to Zorn. *Commentationes Mathematicae Universitatis Carolinae*, 36(1):123–126, 1995.

[10] Joseph Gallian. *Contemporary abstract algebra*. Nelson Education, 2012.

[11] Wilfrid Hodges. Krull implies Zorn. *Journal of the London Mathematical Society*, 2(2):285–287, 1979.

[12] Kenneth Hoffman and Ray Kunze. *Linear algebra*. Prentice Hall Englewood Cliffs, 1971.

[13] Thomas W. Hungerford. Graduate texts in mathematics: Algebra, 1974.

[14] Thomas W. Hungerford. *Abstract algebra: an introduction*. Brooks/Cole Thomson Learning, 1997.

[15] Lloyd Jaisingh and Frank Ayres. *Schaum's Outline of Abstract Algebra*. McGraw-Hill, 2003.

[16] Michael Edward Keating. *A first course in module theory*. World Scientific, 1998.

[17] Wolfgang Krull. Idealtheorie in Ringen ohne Endlichkeitsbedingung. *Mathematische Annalen*, 101(1):729–744, 1929.

[18] Christopher Norman. *Finitely generated abelian groups and similarity of matrices over a field*. Springer, London New York, 2012.

[19] Joseph J. Rotman. *Advanced Modern Algebra*. Prentice Hall, London, UK, 2003.

[20] Jack C. Wilson. A principal ideal ring that is not a Euclidean ring. *Mathematics Magazine*, 46(1):34–38, 1973.

[21] Max Zorn. A remark on method in transfinite algebra. *Bulletin of the American Mathematical Society*, 41(10):667–670, 1935.